



Fischbacher-Smith, Denis, and Fischbacher-Smith, Moira (2014) *What lies beneath? The role of informal and hidden networks in the management of crises*. *Financial Accountability and Management*, 30 (3). pp. 259-278.
ISSN 0267-4424

Copyright © 2014 The Authors

<http://eprints.gla.ac.uk/91104/>

Deposited on: 29 July 2014

What Lies Beneath? The Role of Informal and Hidden Networks in the Management of Crises

DENIS FISCHBACHER-SMITH AND MOIRA FISCHBACHER-SMITH*

Abstract: Crisis management research traditionally focuses on the role of formal communication networks in the escalation and management of organisational crises. Here, we consider instead informal and unobservable networks. The paper explores how hidden informal exchanges can impact upon organisational decision-making and performance, particularly around inter-agency working, as knowledge distributed *across* organisations and shared *between* organisations is often shared through informal means and not captured effectively through the formal decision-making processes. Early warnings and weak signals about potential risks and crises are therefore often missed. We consider the implications of these dynamics in terms of crisis avoidance and crisis management.

Keywords: risk, crisis, informal networks, control, organisational performance

INTRODUCTION

A striking characteristic of organizational life is that there is a lot of talk about decisions, decisions that have been made, are to be made, will be made, should be made, will never be made; talk about who makes decisions, when, how, why and with what results. Organization members interpret a significant part of activities around them in terms of decisions (Laroche, 1995, p. 67).

The processes of decision-making are central to accountability and control within organisations. It is well known, however, that organisations tend to manage what they can measure and that behaviours and reporting alter accordingly,

*The first author is research Professor of Risk and Resilience in the Adam Smith Business School at the University of Glasgow. The second author is Dean of Learning and Teaching in the College of Social Sciences and Senior Lecturer in the Adam Smith Business School at the University of Glasgow. This paper is based on research funded by the EPSRC (Grant EP/G004889/1) and by the Glasgow Centre for Population Health.

Address for correspondence: Denis Fischbacher-Smith, University of Glasgow Business School, Gilbert Scott Building, Glasgow G12 8QQ.
e-mail: denis.fischbacher-smith@glasgow.ac.uk

often to the neglect of important but un-measurable information and activity (Seidl, 2007; and Smith, 2005a). The focus on measurement encourages decision-making that attends primarily to those activities that are known, visible and that can be made explicit. Decision making in relation to risk and risk assessment in particular, has become increasingly prominent in organisations due in part to the reputational damage that can ensue following a crisis and from which organisations have great difficulty recovering (Sipika and Smith, 1993; and Smith and Irwin, 2006). Such assessment relies primarily on calculations of probabilities and the consequences of particular hazards, and this process becomes contextualised within information sharing about organisational risks. This process often relies on experts and senior staff within the organisation to calculate the nature of the risk. These groups draw mainly on hard data or information that is known within the organisation around failure modes and their effects. This information is then shared amongst decision makers. There are, however, several problems with this approach.

Firstly, the process is more effective when the probabilities of failure are known and the consequences are well understood. The approach has problems when it is applied to low probability, high consequence events where the frequency of occurrence is so low or the process is so new that there is uncertainty around the statistical judgements of occurrence (Fischbacher-Smith, 2010). Secondly, there are potential issues around the role that technical expertise can play in the process as powerful interests can serve to distort the assessment of risk under certain conditions (Collingridge, 1992; Collingridge and Reeve, 1986; and Smith, 1990). Thirdly, even where information is available about a particular hazard, the decision-making process can also be shaped by judgement of that risk which is based on informal or more qualitative information. We argue here, that despite the use of such information and expertise, the distribution of knowledge across and between organisations presents significant challenges to organisations in the context of decision-making and risk management because many of the early warnings of crises are shared through informal networks that are both unobserved and potentially unobservable. It is for this reason that organisations often only discover that many of these indications existed about the potential for a crisis after the event. These warnings were either undiscovered until after the event or had been discovered in advance but were not fully understood or prioritised because they did not fit with the decision making paradigm of the organisation (Fischbacher-Smith, 2012). As many of these early warnings exist within intra- and inter-organisational networks, the challenge for management is that of identifying and managing this otherwise hidden information amongst often unobserved and unobservable networks and it is the nature of this challenge that forms the core of the paper.

How information and knowledge informs the decisions that managers make, is something which has been the subject of considerable research interest (Argyris, 1990; Boisot, 1995; Collingridge, 1992; Collingridge and Reeve, 1986;

and Seidl, 2007). Of importance within this literature has been the role of socio-technical networks in shaping the supply of information, verifying and challenging assumptions around decision parameters, and in identifying early warnings of the potential failures associated with particular decisions (Ballinger, et al., 2011; Cross et al., 2006; and Jansen et al., 2011). In many respects, socio-technical networks are a central dynamic of organisational performance, particularly in the context of human services such as healthcare (Doolin, 1999). Here, an organisation's dynamic capabilities (Augier and Teece, 2008; and Barreto, 2010) are a function of the individuals and teams that interact together to deal with the demands of the 'problem space' (Boisot, 1995; and Boisot and Child, 1999) as well as the ways in which the organisation communicates information, structures its knowledge management processes, and develops its staff. The nature of the information and data that is provided, and the processes through which it is analysed and stored, are important elements in shaping how effectively organisations manage this information space and make decisions in the process.

The recent Europe-wide crisis around the contamination of processed foods illustrates the nature of the problem well. In January 2013, beef products in the UK and Ireland, were found to contain significant proportions of horsemeat (Castle and Dalby, 2013; Meikl et al., 2013; Meikle and McDonald, 2013; and Williams, 2013). This horsemeat had made its way into food supplied in hospitals and schools, despite public sector procurement regulations and quality control processes. The subsequent testing by government agencies revealed this to be an endemic problem within the European Union (Leake et al., 2013; Linchfield et al., 2013; and Meikle et al., 2013) and highlighted the difficulties associated with auditing information surrounding the international production and transfer of food products. What became evident from the early stages of this crisis was that financial drivers were a key factor in shaping behaviours in a globalised supply chain. The crisis also illustrated the problems associated with a weak regulatory framework (or at least one that was weakly enforced) and a range of issues around auditing compliance. The horsemeat crisis was not the only event to illustrate problems around regulation and compliance. The death of patients at mid-Staffordshire hospital (in the UK) (Francis, 2010), the so-called 'horsemeat scandal' (Castle and Dalby, 2013; Leake et al., 2013; and Thomson, 2013), and the presence of non-clinical grade silicone in breast implants (Berry and Stanek, 2012; and Freshwater, 2012) also highlighted the problems around accountability and control against a backdrop of economic pressures.

In human services, such as health care, where organisations are heavily dependent on their human capital to achieve effectiveness, knowledge, information, data and decision making can be seen as being largely co-produced with other organisations involved such as social care, education, and third sector agencies providing social support (Osborne, 2006 and 2009). As such, the quality of the human, relationships between service providers (which are often informal), and between these providers and their consumers

(or patients) also significantly influences the nature of organisational performance and effectiveness. Much of the literature on service provision emphasises these interactions in terms of improving service integration, strengthening inter-agency cooperation, and clarifying protocols between agencies so as to reduce gaps in service provision. Some stimulus for this has arisen out of cases concerning child protection and older people's services, especially those where the system was deemed to have failed a vulnerable child or older person. Such services have often provided a focus on the difficulties associated with this network of co-production especially in relation to communicating problems or near misses, or following up on concerns as early warnings. Both children's and older people's services are particularly good examples because protection and care depends almost entirely on effective inter-agency (health and social-care) working. Information flows and knowledge management are thus often identified as processes where failures can occur around early warnings and near-miss events (Rasmussen, 1982 and 1983; Reason, 1990 and 1997; and Turner, 1976 and 1978). Within this literature, however, little attention has been given to the substantial limitations organisations have in controlling informal information sharing and decision making between networked organisations and thus the vulnerabilities networks can create.

Our aim here, therefore, is to consider how networked service organisations rely on informal human interaction as an essential conduit of information and knowledge exchange, and to illustrate how these interactions often remain unobservable and uncontrollable by managers, thus having significant potential to directly cause and/or escalate crises. Drawing on both inter-organisational theory and the extensive body of work in crisis management, we examine how vulnerability may be created and early warnings ignored and we consider the implications of informal networks for managerial intervention, contingency planning, and managerial control. Before exploring these processes further, we first need to outline some of the key factors around the management of risk and the limitations of control.

RISK, CONTROL AND UNOBSERVABILITY

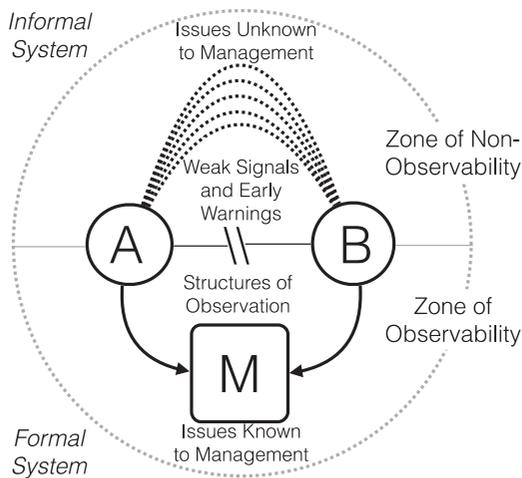
Risk is typically understood in terms of estimating both the likelihood and the consequences of a particular event occurring (see for example, Royal Society, 1983 and 1992). Risk management is concerned with the processes of identifying areas of potential hazard, reducing the probability of their occurrence and mitigating the remaining potential vulnerability that exists in relation to that risk. Residual risks are ideally removed, or if that is not possible, then the potential losses are insured. In terms of contingency planning for risk, well-prepared organisations will develop policies to deal with a range of hazards from 'natural', through technological accidents, to malicious or erroneous damage caused by the actions of employees or external agents. Such policies invariably seek to ensure a coordinated, efficient and effective response to situations that

arise, and staff will be trained (to some extent) to respond to such situations (Smith, 2000 and 2004).

An important consideration within the risk management process is how the activities and information flows that occur within the organisation are controlled through the (risk) management function and the limitations associated with that process. Figure 1 shows the relationship between three employees: a manager (designated as ‘M’) and two members of staff (‘A’ and ‘B’). A great deal of management theory and practice tends to assume that sufficient information will be captured through formal processes, and that early warning signals about potential problems will also be captured in this way (Brookfield and Smith, 2007). As such, this conforms what Seidl terms the ‘structures of observation’ – which leads to those elements of organisational performance that are observed (the zone of observability) and those that are effectively ignored (the zone of non-observability) (Merton, 1957; and Seidl, 2007). These ‘structures of observation’ involve two considerations: the first concerns how such structures can shape observations and the second concerns how these observations relate to each other across time and place (Seidl, 2007). Knowledge also provides the mechanism by which certain observations are excluded and Seidl argues that:

knowledge is a selection of certain (generalized) distinctions for observation from all possible ones. Thus, the reverse side of knowledge is an *exclusion* of distinctions for observation; an exclusion of possibilities of observation (Seidl, 2007, p. 20).

Figure 1
Elements of Organisations



Management will invariably seek to shape the nature of observations and the processes around knowledge creation and transfer. Invariably, this is seen as taking place through formal managerial processes and the bureaucratic functions of the organisation, rather than through any informal processes. In reality, however, a considerable amount of information is exchanged informally between employees and may bypass formal management mechanisms/functions.

The logical extension of this argument is that at any point in time, managers will have incomplete information around discussions pertinent to risk and, more importantly, may fail to identify information that would point to early warnings of impending failure. In some respects, these early warnings may be missed as a result of what Seidl (2007) terms non-knowledge and the exclusion of certain forms of observation. Similarly, the leakage of information and knowledge outside of the organisation can bypass existing control mechanisms and be used to generate harm for the organisation through direct and malicious actions by outsiders. The insider threats are increasingly seen as important due to the threats from espionage (both commercial and state), terrorism, and organised crime. Inevitably, such processes are also (or aspire to be) invisible to detection and therefore also to management. When one considers that there is a normal degree of misbehaviour within organisations such as bending rules, cutting corners, bypassing 'unnecessary' bureaucracy (see Ackroyd and Thompson, 1999), then it requires little imagination to see how intentional harm may be caused by those with malicious intent seeking to exploit weaknesses.

Although managers are likely to want to create structures where they themselves become the key connector between individuals, in reality, situations are more complex for various reasons. Firstly, and particularly in healthcare, multidisciplinary teams, integrated services and managed clinical networks for example, all require team-wide formal communications and the ability of team members, who may not all be employed by one organisation, to take devolved decisions along the lines of their professional training, autonomy and judgement. It may be, for example, that a social worker and community psychiatric nurse (employed by the NHS and Council/Local Authority respectively) need to undertake a joint visit to a patient in the patient's own home. Their decision making will be influenced by their training, the particular circumstances, the health and wellbeing of the patient, any informal 'modus operandi' that the two individuals have reached after working together over time, any relationship of trust, and prior knowledge of the patient or locality. Such dimensions do not fall within the structures of observation to any great extent despite the role of formal inter-agency protocols and the extensive documentation of visits and assessments.

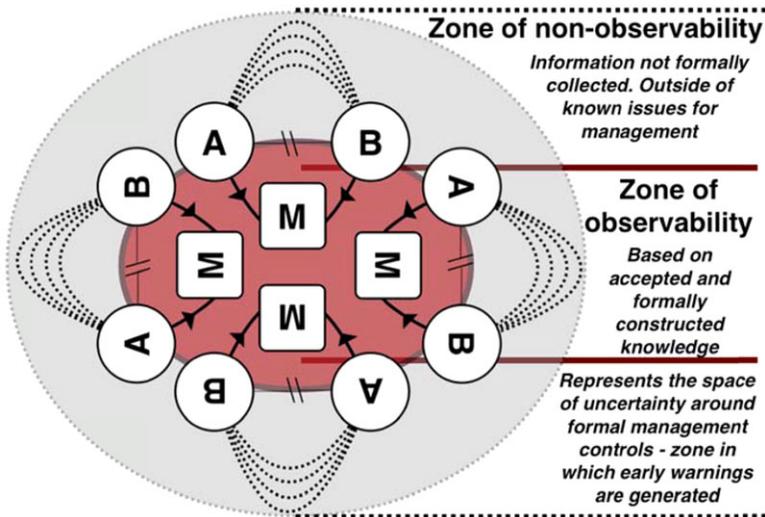
Their manager(s) will be geographically and temporally remote from that decision so will have limited control over the nature of their interaction, little opportunity to identify the existence of an informal relationship between them and therefore, limited opportunity to capture the information shared. In the majority of cases, this will not give rise to a crisis and whilst it may render the

manager a less socialised perspective of their own area of responsibility, day to day service may be provided to a high level and patient needs met. However, there are sadly cases where difficulties arise and crises do emerge. One need only read the newspapers to hear frequently of cases where a patient has injured someone, where the patient was known to health and care services and where, ‘poor communication’ is deemed to have allowed the situation to occur and indeed to escalate to the point that it has. The issue then is how, and indeed if, it is possible for a manager to ever be able to capture or ensure that key knowledge in a situation like that is communicated and acted on appropriately.

When multiplied to consider the exponential number of informal relationships within and between organisations in which risk-related issues might be communicated, the challenge to organisations and their managers dealing with risk grows significantly. Figure 2 captures the formal risk analysis processes between teams (within or between organisations). It also identifies the informal communications (dotted lines between A and B) and the way in which they feed into wider sets of informal network communications they engage in.

The challenge for organisations is that where multiple departments or organisations are linked together, the focus is normally on formal risk analysis processes which will, in turn, be based on the structures of observation that are in place within the organisation(s) involved in delivering a service or responding to a crisis where it occurs. The structures of observation will help to shape perceptions of the range of anticipated events and any worst-case scenario. The

Figure 2
 Knowledge Transfers Around Early Warnings



outer interactions within Figure 2 are largely of an informal nature and may capture information that is present within the zone of non-observability. As the informal networks extend beyond the span of formal controls, early warnings (often fairly weak signals) are not likely to be identified in an effective manner.

Many of the information flows and communication processes that take place within organisations occur informally. Colleagues share with their peer groups the shortcomings of processes, the inadequacy of information, the limitations of data, the distortions within management information systems, and yet often, managers themselves are unwilling to acknowledge such shortcomings and so do not recognise the potential for failure. Interactions between individuals 'A' and 'B' are typically interpreted by managers through the lenses of formal organisational structures and formal reporting mechanisms, to the neglect of the informal, yet, as the dotted lines in Figure 1 denote, it is likely that there will be multiple informal communications between 'A' and 'B', and these potentially transcend formal boundaries as discussed above. Bureaucratic processes will therefore inevitably fail to capture the detail of early warnings and will often prove to be too slow to react when these warnings are captured. They may also be unable to contain the flow of sensitive information outside of the organisation. Overly-bureaucratic environments may also cause individuals to violate (in order to get the job done), thereby moving the organisation closer to the potential for failure whilst allowing managers to believe that their perceived higher levels of controls will guarantee increased safety (Ackroyd and Thompson, 1999; Reason, 1990 and 1997; Weick, 2001; and Weick and Sutcliffe, 2001).

This process is shown in simplified manner in Figure 2, where a set of interactions take place that lie outside of the normal sphere of managerial control and which generate a perception of order in a situation where the reality is disorder. It is within these informal relations that a great deal may be discussed about the organisation, about the range of tasks and activities undertaken (e.g., discussion of management's approach to a particular project) and that will thereby generate considerable potential for sharing essential knowledge about hazard and risk. The organisation's inability to capture this information will inhibit its ability to prevent crises as this informal system is an essential transmitter and creator of knowledge around risk. Unfortunately, the formal processes surrounding risk assessment will often not take account of these informal networks (as a source of early warning information) as they sit outside of the structures of observation imposed by the organisation. Thus, early warnings and weak signals shared within these informal networks will not be captured by the organisation. In response to these problems and information asymmetries, many organisations seek to add multiple layers of controls and build further redundancy into the system in order to prevent failures from escalating. However, not only can such approaches bring with them problems around the escalation of risk (through processes of emergence) but they serve to make the system more opaque and therefore more difficult to manage. These additional layers of control are also no better able to deal with unobservability.

If systems designers and those involved in managerial and accounting control functions do not consider certain elements to be important then they will remain marginalised and essentially unobserved. During the horsemeat crisis in the UK, for example, a senior manager within a large food retailer observed that the industry does not routinely check for the DNA of some animals and so its presence or absence is never verified. Many organisational controls are based on such assumptions. The underlying problem of hidden networks of knowledge therefore remains.

A NETWORK PERSPECTIVE ON CRISES AND VULNERABILITY

The myriad relationships perpetuated by globalisation and by government approaches to involving private sector providers in the delivery of public services mean that all aspects of the design, delivery, management and measurement of product and service delivery ultimately need to be considered from a network perspective (Kickert et al., 1997). Organisational performance is deemed to be improved through the increased flexibility and responsiveness afforded by carefully designed inter-organisational relationships and by improvements in the transparency, auditability and governance of information within that process (de Bruijn, 2007). Other alleged benefits include quicker decision making processes, improved communications and a reduced emphasis on command and control. A concomitant focus on core business activities and efficient means of delivery has frequently resulted in efficient internal and external networks that allow for 'just in time' delivery and lean production. Better integration is thought to reduce duplication, improve the efficiency of resource allocation and resource utilisation, and to ensure that decisions are taken close to the consumer, i.e., at the locus of service provision.

Paradoxically, the same networks that generate these efficiencies for organisations in terms of the speed of interaction and the extent of the supply chain, also generate problems. Networks have brought with them the potential for failures to migrate quickly through the 'tightly coupled' and 'interactively complex' (Perrow, 1984) nature of the organisation as a system. In this way, 'just-in-time' processes can easily become 'just-too-late' (Smith, 2005b) as organisations no longer have the resource slack that they need to deal with surges in task demands. The capacity of a regional health authority to respond to a disease outbreak or a major incident, for example, is often largely contingent on its resource slack, and the effectiveness of its emergency planning arrangements with other agencies. Where the communication of information, decision-making, the utilisation of resources, and the network infrastructures that support them are inefficient or ill informed, then an existing crisis can escalate quickly across that system and exceed the capabilities of service providers to deliver what is necessary despite contingency arrangements (Smith, 2005a).

The central role of public-private supply chain networks within a highly globalised industry raises some significant challenges for public management

regulatory systems, especially in a period of intense cutbacks and austerity. What is clear from a consideration of several crises in recent years is that any weaknesses in state regulatory systems at the national level can have a major impact on vulnerabilities within the single market of the European Union. As this economic trading block increases its membership and given the differential impacts of the economic downturn across this economic landscape, we should not be surprised that the various state regulatory agencies differ in terms of their performance. Clearly, the contamination of the food chain by horsemeat is indicative of this problem.

The emergence of the breast implant case in late 2011 and early 2012 also illustrated how the interconnected nature of organisations can generate problems, in this case, arising from unethical behaviours, to have a deleterious effect on other organisations in the network. The use of non-medical grade silicone by the French-based company PIP and the subsequent concerns of women who had them fitted, resulted in a crisis that spread throughout Europe and internationally (Keogh, 2012). In the UK, the crisis prompted a government assessment of the safety of PIP implants (Keogh, 2012) and, despite the low level of calculated risk, there was considerable pressure placed on private providers to remove implants (O'Dowd, 2011a and 2011b; and Templeton and Follain, 2012). As many of these implants were part of a cosmetic procedure, they were carried out privately. For those implants carried out by the NHS, an undertaking was given to replace them.

Both cases also illustrate the impacts of a de-regulation culture and an associated erosion of regulatory capability around monitoring and enforcement. Within an age of austerity, this erosion of regulatory capability can be seen to decrease the chances of the state being able to detect violations and may, at the same time, increase the pressures on organisations within the supply chain to violate in an attempt to maximise profitability. Within such a context, warnings around violations are more likely to emerge from informal networks and whistleblowing rather than through inspection regimes. The deaths at mid-Staffordshire hospital serve as an illustration of the failures in regulatory processes to identify poor performance around patient safety and to learn effective lessons from such events (Francis, 2010; Ocloo and Fulop, 2012; and Reid and Catchpole, 2011). Both the PIP and horsemeat contamination examples also illustrate the role of trust within the regulation of risk across extended supply chains and networks. At the core of this is how receiving elements within a supply chain assume that the products received into their own processes meet the standards required. Invariably, this involves some degree of trust between members of the supply chain network; often supported by informal relationships that evolve over time.

The challenge for public management is therefore how to leverage informal networks when the formal regulatory mechanisms are degraded and how to understand and manage the informal dimension of inter-organisational networks so as to minimise their vulnerabilities. Yet our understanding and

management of formal and informal networks and network performance is demanding both conceptually and practically, meaning there is as yet, limited research-based insight for public managers to draw upon in practice. Attention has typically been given to aspects of inter-agency collaboration such as sustaining collaborative effort, achieving collaborative advantage and evaluating the success of such endeavours (Head, 2008; Huxham and Vangen, 2005; Jaaskelainen and Lonnqvist, 2011; and Rodan and Galunic, 2004) rather than with the management of informal networks and their impact on the generation and migration of crises across organisations, spaces and places.

Socio-technical networks generally, and informal networks in particular, are not routinely seen as a source of vulnerability and much of the literature emphasises the benefits derived from social interactions and relationships. These include the rapid dissemination of information, the communication of tacit knowledge, potential improvements in organisational performance, and the ability to quickly galvanize interest and support where networks are supported by communications structures (Borgatti and Foster, 2003; and Gnyawali and Madhavan, 2001).

There is, therefore, a double-edged aspect to socio-technical networks: they can both allow risks to escalate and can provide organisations with a degree of resilience around crisis prevention. The more resilient an organisation can become, the more effective it should be in picking up on, and dealing with, early warnings. It becomes important therefore to understand how such hazards, and the risk of these hazards, can be affected by, and also affect, socio-technical networks within and between organisations. However, as we go on now to explore, much of the interaction within socio-technical networks is informal and frequently hidden presenting significant challenges to managers and accountants seeking to ensure transparency, probity and accountability.

HIDDEN AND INFORMAL NETWORKS

Networks transcend formal organisational boundaries and formal means of observation and control. They are also usually characterised by elaborated codes (Bernstein, 1966) representing the language used by expert groups within the network. These codes are often impenetrable by those outside of the expert group and serve as a barrier to discourse. At its core, knowledge is constructed (or rejected) as a function of how we make sense of what we 'observe' in the world around us (Weick, 2001; and Weick and Sutcliffe, 2001). We tend to select or accept information that suits our needs, and that we recognise as relevant to our interests (Boisot, 1995; Collingridge and Reeve, 1986; and Taylor, 2000). In part, this sensemaking process is shaped by the values and core beliefs that we hold. For example, in a healthcare setting, clinical staff may readily identify and accept information that reinforces their views on particular approaches to patient care, but be much less receptive to (and thus pay less attention to)

information about cost, purchasing options or managerial incentives. As Powell observes:

The most useful information is rarely that which flows down the formal chain of command in an organisation or that which can be inferred from shifting price signals. Rather, it is that which is obtained from someone whom you have dealt with in the past and found to be reliable. You trust best information that comes from someone you know well (Powell, 1991).

Thus, informal networks may become powerful conduits of knowledge that is often deemed to supersede or negate organisationally-produced knowledge. Such exchanges are, however, largely hidden and thus evade the normal management and control processes within organisations.

Seidl (2007) argues that observation and knowledge are linked but they are not the same thing:

... knowledge is something that *guides* observation. That is, it is something that in the concrete moments of observation provides an orientation for where to draw the distinction. In that sense, we can parallel knowledge with *structures of observation* (Seidl, 2007, p.19).

How we define and frame a problem will largely determine how we observe and perceive it and this will, in turn, shape our response to it. Informal networks can, however, allow for 'non-knowledge' (Seidl, 2007) to be challenged, as evidence from other contexts and other perspectives is brought to bear on the constrained observations that are codified *within* organisations. Professional bodies are a key conduit for this process as they provide a range of mechanisms for information sharing and networking. The issue then becomes one of whether the organisation absorbs and responds to this knowledge. The interactions between individuals generate a set of connecting fabrics that both exist, and are perpetuated beyond, the control and sphere of any single organisation.

In these 'spaces', knowledge is created and disseminated and serves to shape the views and behaviours of individuals within the network. This, in turn, creates social capital and knowledge that is the possession of the individual (and the network) and not, necessarily, their employer. Not all of this information is necessarily actionable. For example, local authority education staff who deal with vulnerable children come to know the children's circumstances well, often develop informal ties with staff in related agencies such as healthcare, social care, schools and the police. This is particularly the case around those families where there are anti-social behaviour or addiction problems such that families are brought into contact with multiple agencies. During informal exchanges, background information is often passed between individuals that is not officially permissible (due to client confidentiality) but which front line staff value and deem necessary to effectively undertaking their role. Such communications can result in interventions (under other auspices) that avert a potential crisis. It is also conceivable though that within the network space there is also the

potential for disinformation and failure as the knowledge communicated may be inaccurate, decontextualized, or out of date, thereby leading to inappropriate actions. Such failures can migrate quickly and create multiple 'pathways of vulnerability' (Smith, 2005b) in which the potential for failure can be embedded and remain undetected across a range of connected organisations. These pathways are an extension of Turner's (1976 and 1978) notion of incubation and Reason's (1990) resident pathogens by elevating the importance of space, place and time in both the generation of failure (failure modes and probabilities) and its 'complexion' (failure consequences and cascades). If we consider the failures that can be generated within (supply chain) networks then it is possible to see organisations as having multiple 'pathways of vulnerability' embedded within their sphere of operations. Many of these pathways will originate outside of the organisation's formal boundaries but will have consequences within them. Informal networks are, therefore, an important but essentially neglected element of an organisation's risk portfolio as there is a largely under-explored 'dark side' to them.

DECISION MAKING: DEVELOPING CONTINGENCIES AND MANAGING CRISES

The managerial limitations we have highlighted so far create both intra- and inter-organisational vulnerabilities. The gaps in knowledge combined with an inability to observe and control much of the communication and knowledge concerning technical and non-technical issues, will serve to create holes in organisational defences. Reason (1990) argues that these gaps may become aligned with gaps in other parts of the organisation, creating vulnerabilities at a number of levels within the organisation. Where gaps become aligned due to the range of issues noted previously with regards to information, communication, error reporting behaviours, hierarchy and so forth, then latent error pathways are created such that hazards can permeate through the organisation(s) and its networks, thereby creating significant losses in terms of control, reputation, and service provision. At its worst in a healthcare context, this means an adverse event in hospital, failure to respond to a community crisis on time, poor diagnosis and inappropriate pathways of care or the death of a patient or innocent victim (Fischbacher-Smith and Fischbacher-Smith, 2009). A multi-agency network thus potentially incubates a significant risk of destabilising a number of organisations simultaneously or in a domino effect. As a consequence of these non-observed networks, there will be information about the various risks that are generated as part of the organisation's activities that is not captured by managerial control systems i.e., through the formal processes. The essential issue here is that at any point in time, the risks that are identified and measured within a formal process will represent only a proportion of the hazards that are faced by the organisation.

There are important implications for contingency planning given this line of argument. Organisations' contingency planning processes will generally be

based on the formal interactions that are measured and managed. Senior staff who typically develop contingency responses, will rely on formal information and data analysis to calculate capacity and to determine a portfolio of risks, typically informed by a local risk register. Informal communications amongst those who deliver services, may present quite different accounts of capacity, knowledge, understanding, decision making and communication pathways that will render some contingency planning assumptions invalid. This means conditions may arise that move the organisation beyond its contingency limits and outside of the scope of the plans that are put into place to deal with serious adverse events (Smith, 2005a). Thus, although it is often assumed that the identification of risk and the development of associated contingency plans is largely sufficient to deal with any ensuing crisis or hazardous situation, it is more likely to be the case that there will be various circumstances in which this proves to be a grossly inadequate assumption. It is not unlikely given our argument above, that a healthcare provider would quickly find that many of its assumptions were inadequate during contingency planning activities and that a crisis situation therefore quickly escalates beyond the contingency limits. Moreover, given the networked nature of organisations, as the PIP case illustrates, events combine and create emergent conditions that are unexpected and uncontrolled, taking the organisation(s) beyond anticipated and controlled limits.

It is at this point that we again recognise the dual role of informal networks. When the organisation is dealing with issues that have been anticipated and are within the scope of the contingency response, they will marshal teams of staff, commandeer equipment and take up residence in premises within their control centres to house crisis teams. The level of mobilisation will vary between organisations and there will be a concerted process of monitoring and evaluation that is aimed at preventing the 'event' from escalating further (Smith, 2000 and 2004). The extent of this crisis management process will, of course also be shaped by the 'structures of observation' (Seidl, 2007) that are in place. At this stage, one of two things may occur. The event may escalate but nonetheless retain certain characteristics that are conceivable within the dominant paradigm, although this does not make them readily manageable. It is also the case, however, that scenarios may occur that challenge the dominant paradigm within the organisation. They may not have been accepted by management prior to the crisis (e.g., the idea that NHS doctors might commit a terrorist attack), as the evidence-base to support such a challenge had not been accumulated by the formal processes. In both situations, informal networks can play an important role in allowing crisis management team members to leverage the knowledge and resource bases that exist within their informal networks and to alleviate the crisis, preventing further escalation. These informal networks could provide management with (indirect) access to expertise and knowledge held by people outside of the formal crisis teams. A key consideration will also be the ability of informal networks to challenge the organisational paradigm

following the event. It will be interesting to see how the medical devices sector responds in the wake of the PIP case and increasing calls for a tighter regulatory enforcement regime.

HUMAN NETWORK CHALLENGES TO MANAGERIAL CONTROL

How organisations manage the knowledge that is present within their control, and how they deal with the more informally generated knowledge that exists within the hidden networks that permeate the organisation is an essential consideration. It is increasingly the case that organisations must be sensitive to both internal and external signals, and as a consequence must find a means of capturing information throughout and beyond the organisation. An effective transfer of knowledge between organisational members, along with the challenges made to core assumptions in the process, should allow for a more effective crisis response capability, especially around early warnings. Such a perspective invariably takes the view that the essential knowledge needed to run the organisation is distributed across the organisation and is not just concentrated at the senior management level of the organisation.

Another important aspect of informal, hidden networks is that highly sensitive information that is essential to organisational performance may find more opportunities for 'leakage' or, in some cases, early warnings of problems might not be picked up by those who are in a position to take action to prevent escalation. The development and maintenance of lines of communication between members of the organisation, needs therefore, to be a key focus of managerial attention. Whilst many organisations would agree with this, there are several important barriers to effective implementation, especially when dealing with issues around risk.

Firstly, risk assessment by its very nature involves predicting the likelihood of an event occurring and taking subsequent steps to mitigate those risks. Prediction is based on both known and unknown factors, and thus the organisation's ability to capture relevant information and make informed judgements on which to base their predictions, becomes essential. Much of this information is, however, complex and requires interpretation and analysis by experts. Much of it also lies within the zone of unobservability, exchanged within hidden networks. This interpretation may, under certain conditions, generate the potential for future risks as the decisions taken on the basis of a flawed perspective will serve to shape the control methods put into place.

A second issue, and one that is also important in relation to issues of expertise, is the hierarchy within which information is collated, shared, analysed and disseminated. If error reporting is initiated by a relatively junior member of staff within an organisation that is characterised by professional hierarchy, then the problems of authority gradients can be a significant factor in preventing information flows and subsequent action. Such hierarchies are common to a range of industries such as healthcare, engineering and

airlines. In some circumstances the power-dynamics within organisations can mean that errors are either not reported (as frontline, junior, staff may feel unable to challenge higher level decisions), or are ignored because the reporter is deemed to be inexperienced or a non-expert. Yet again, the issues will commonly be well-known and communicated among informal but hidden networks.

A third issue concerns the problem associated with constrained boundaries of consideration amongst decision makers who tend not to consider issues beyond the short term. They prioritise the requirement to deal with immediate problems at the expense of the possible long-term cost. These factors, combined with the issues around determining the legitimacy of knowledge and the social construction of risks, generate challenges to the ways in which organisations deal with risk and crisis. The problem becomes compounded when we consider the impact of such problems *across* the multi-organisational networks that characterise public services such as health and social care. What is less comprehensively acknowledged is the significance that these issues will have within the wider inter-organisational context in which both risk and crisis occur and are transmitted (Smith and Irwin, 2006). A crisis may no longer be confined to one organisation and there is a clear potential inter-agency effect as organisations become more tightly coupled (Perrow, 1984) to each other through complex supply chain networks. What is becoming increasingly clear as a result is:

that in a highly interconnected world, the actions of other organisations may also play an important role in the development and migration of crisis potential (Smith and Barton, 2007, p. 65).

Thus, it is also the case that the ability of one organisation to respond to a crisis situation will potentially enable or disable others within the network, as supply and value chains generate the potential for common mode failures or as critical national and international infrastructures become vulnerable to external attack and failures (Boin and Smith, 2006). The issues here also relate to the limits of managerial control across boundaries and to the interaction effects of one organisation's performance on another under conditions of crisis. The latter relates very much to the collective capacity of inter-connected organisations – the ability to perform in what Kauffman terms a 'fitness landscape' (Kauffman, 1993), but such issues go beyond the scope of this paper.

CONCLUSIONS

Our aim in this paper has been to set out the problem space for information capture and analysis within organisations. We have tried to frame the information terrain in terms of what is measured (because that is invariably what is managed) and what is unobserved. It is these unobserved spaces that generate the dark territory within organisations and which serve to allow crises

to be generated. In the crisis of legitimation that follows every crisis, it is invariably the unobserved aspects of the organisation that are held up as key factors in shaping the evolution and escalation of the crisis. Often these issues, unobservable interactions and knowledge exchanges will have conveyed some form of early warning but the warning will have been missed or rejected as having little or no importance in determining organisational performance. The concerns expressed within informal networks are thus strangled at birth by a formal system that both fails to recognise their significance and is almost incapable of dealing with them because no structures and processes are available to 'manage' them. Even after a crisis, organisations often display a degree of paradigm blindness towards the issues (Fischbacher-Smith, 2012).

Organisations embody informal relationships that are beyond their physical, political, economic, and managerial boundaries. They are, therefore beyond managerial control and yet significantly influence organisations acting individually and collectively. Although informal networks are hugely beneficial in terms of organisational performance, especially in complex systems such as healthcare, the problems associated with structures of observation are significant. They are also likely to be compounded *across* organisational boundaries, yet there has been relatively little consideration of how informal networks may have the capacity for self-harm through quickly transmitting errors via uncontrolled social means of communication. Similarly, there has been little attention on how they might create vulnerabilities for the organisations who are embedded within a set of tightly-coupled linkages.

As economies move increasingly towards mixed forms of public, private and third sector provision of public services, it is essential that this interconnectivity is recognised and understood. Given that organisations will seek to perform at optimal levels, their ability to identify and manage error or hazard potential is crucial. In their attempts to do so, informal networks become significant to the performance of individual organisations. Where network communications are inadequate, informal networks will exacerbate individual organisations' vulnerabilities such that the network as a whole contains penetrable layers of vulnerability.

This paper has argued that the limits to managerial control within organisations are such that the informal networks between individuals within and across organisations may serve to bypass established internal systems designed to reduce the organisation's vulnerability to external hazard. The challenge for professionals and managers within organisations is, therefore, to recognise and reconceptualise the destructive capacity of informal networks (the 'dark' side of networks), particularly in light of the non-knowledge or unobservable transmission of information that is nonetheless strategically and operationally essential to organisations in terms of protection and mitigation of risk. The argument is not intended to negate the role of managers or to suggest that efforts to identify and manage a risk portfolio are fruitless. Rather, we propose that the mindset towards sources of risk be adapted to recognise the vulnerabilities

that (could) exist within an organisation's set of network linkages. Moreover, we suggest that managers recognise the vulnerabilities generated due to non-knowledge such that greater awareness is created within organisations of the potential for informal networks to identify and generate risk. We also argue that in considering organisational responses to crisis situations, that crisis management strategies take more conscious account of the inter-dependence of organisations, and the extent to which the underperformance of one organisation within the network, may be detrimental to the survival of others.

REFERENCES

- Ackroyd, S. and P. Thompson (1999), *Organizational Misbehaviour* (London: SAGE).
- Argyris, C. (1990), *Overcoming Organizational Defences. Facilitating Organizational Learning* (Englewood Cliffs, NJ: Prentice Hall).
- Augier, M. and D. J. Teece (2008), 'Strategy as Evolution with Design: The Foundations of Dynamic Capabilities and the Role of Managers in the Economic System,' *Organization Studies*, Vol. 29, pp. 1187–208.
- Ballinger, G., E. Craig, R. Cross and P. Gray (2011), 'A Stitch in Time Saves Nine: Leveraging Networks to Reduce the Costs of Turnover,' *California Management Review*, Vol. 53, pp. 111–33.
- Barreto, I. (2010), 'Dynamic Capabilities: A Review of Past Research and an Agenda for the Future,' *Journal of Management*, Vol. 36, pp. 256–80.
- Bernstein, B. (1966), 'Elaborated and Restricted Codes: An Outline,' *Sociological Inquiry*, Vol. 36, pp. 254–61.
- Berry, M. G. and J. J. Stanek (2012), 'The PIP Mammary Prosthesis: A Product Recall Study,' *Journal of Plastic, Reconstructive & Aesthetic Surgery*, Vol. 65, pp. 697–704.
- Boin, A. and D. Smith (2006), 'Terrorism and Critical Infrastructures: Implications for Public-Private Crisis Management,' *Public Money and Management*, Vol. 26, pp. 295–304.
- Boisot, M. (1995), *Information Space* (London: Thompson Business Press).
- and J. Child (1999), 'Organizations as Adaptive Systems in Complex Environments: The Case of China,' *Organization Science*, Vol. 10, pp. 237–52.
- Borgatti, S. P. and P. C. Foster (2003), 'The Network Paradigm in Organizational Research: A Review and Typology,' *Journal of Management*, Vol. 29, pp. 991–1013.
- Brookfield, D. and D. Smith (2007), 'Managerial Intervention and Stability in Healthcare Organisations: The Role of Complexity in Explaining the Scope of Effective Management,' *Risk Management: An International Journal*, Vol. 8, pp. 268–93.
- Castle, S. and D. Dalby (2013), 'Horse Meat in Food Stirs a Furor in the British Isles,' *The New York Times* (8 February) (Accessed on line at 2003 hours on the 12th February, 2013).
- Collingridge, D. (1992), *The Management of Scale: Big Organizations, Big Decisions, Big Mistakes* (London: Routledge).
- and C. Reeve (1986), *Science Speaks to Power: the Role of Experts in Policy-Making* (London: Francis Pinter).
- Cross, R., T. Laseter, A. Parker and G. Velasquez (2006), 'Using Social Network Analysis to Improve Communities of Practice,' *California Management Review*, Vol. 49, pp. 32–60.
- de Bruijn, H. (2007), *Managing Performance in the Public Sector* (Abingdon, Oxon: Routledge).
- Doolin, B. (1999), 'Sociotechnical Networks and Information Management in Health Care,' *Accounting Management and Information Technologies*, Vol. 9, pp. 95–114.
- Fischbacher-Smith, D. (2010), 'Beyond the Worse Case Scenario. 'Managing' the Risks of Extreme Events,' *Risk Management: An International Journal*, Vol. 12, pp. 1–8.
- (2012), 'Getting Pandas to Breed: Paradigm Blindness and the Policy Space for Risk Prevention, Mitigation and Management,' *Risk Management: An International Journal*, Vol. 14, pp. 177–201.
- and M. Fischbacher-Smith (2009), 'We May Remember, But What Did We Learn? Dealing With Errors, Crimes and Misdemeanors Around Adverse Events in Healthcare,' *Financial Accountability & Management*, Vol. 25, pp. 451–74.

- Francis, R. (2010), *Independent Inquiry into Care Provided by Mid Staffordshire NHS Foundation Trust January 2005-March 2009*, Vol. 375 (London: The Stationery Office).
- Freshwater, M. F. (2012), 'The PIP Crisis: Déjà vu All Over Again?' *Journal of Plastic, Reconstructive & Aesthetic Surgery*, Vol. 65, pp. 840–43.
- Gnyawali, D. R. and R. Madhavan (2001), 'Cooperative Networks and Competitive Dynamics: A Structural Embeddedness Perspective,' *The Academy of Management Review*, Vol. 26, pp. 431–45.
- Head, B. W. (2008), 'Assessing Network-Based Collaborations. Effectiveness for Whom?' *Public Management Review*, Vol. 10, pp. 733–49.
- Huxham, C. and S. Vangen (2005), *Managing to Collaborate. The Theory and Practice of Collaborative Advantage* (London: Routledge).
- Jaaskelainen, A. and A. Lonnqvist (2011), 'Public Service Productivity: How to Capture Outputs?' *International Journal of Public Sector Management*, Vol. 24, pp. 289–302.
- Jansen, R. J. G., P. L. Curseu, P. A. M. Vermeulen, J. L. A. Geurts and P. Gibcus (2011), 'Social Capital as a Decision Aid in Strategic Decision-Making in Service Organizations,' *Management Decision*, Vol. 49, pp. 734–47.
- Kauffman, S. A. (1993), *The Origins of Order. Self Organization and Selection in Evolution* (New York: Oxford University Press).
- Keogh, B. (2012), 'PIP Breast Implants: Interim Report of the Expert Group' (Department of Health, London).
- Kickert, W. J. M., E.-H. Klijn and J. F. M. Koppenjan (1997), *Managing Complex Networks. Strategies for the Public Sector* (London: Sage Publications).
- Laroche, H. (1995), 'From Decision to Action in Organizations: Decision-Making as a Social Representation,' *Organization Science*, Vol. 6, pp. 62–75.
- Leake, J., J. Ungoed-Thomas and G. Graham (2013), 'No Checks for Horse DNA in 10 Years,' *The Sunday Times* (10 February, p. 8).
- Linchfield, J., D. Randall and S. Manning (2013), 'IoT Investigation: Horsemeat Scandal Reveals Trail of Shadowy Suppliers,' *The Independent* (10 February) (Accessed on line at 1933 hours on the 11 February, 2013).
- Meikle, J. and H. McDonald (2013), 'Tainted Meat in Store Not Our Product, Says Newry Firm,' *The Guardian* (6 February, p. 12).
- , J. Buckley and F. Lawrence (2013), 'Horsemeat Could Have Been Present in UK Burgers for More Than a Year,' *The Guardian* (31 January, p. 15).
- Merton, R. K. (1957), 'The Role-Set: Problems in Sociological Theory,' *The British Journal of Sociology*, Vol. 8, pp. 106–20.
- O'Dowd, A. (2011a), 'French Women to Have PIP Breast Implants Removed for Free,' *BMJ*, Vol. 343.
- (2011b), 'UK Recommends PIP Breast Implants Should Not be Removed,' *BMJ*, Vol. 343.
- Ocloo, J. E. and N. J. Fulop (2012), 'Developing a "Critical" Approach to Patient and Public Involvement in Patient Safety in the NHS: Learning Lessons From Other Parts of the Public Sector?' *Health Expectations*, Vol. 15, pp. 424–32.
- Osborne, S. (2006), 'The New Public Governance?' *Public Management Review*, Vol. 8, pp. 377–88.
- (2009), 'Delivering Public Services: Are We Asking the Right Questions?' *Public Money and Management*, Vol. 29, pp. 5–7.
- Perrow, C. (1984), *Normal Accidents* (New York: Basic Books).
- Powell, W. W. (1991), 'Neither Market nor Hierarchy: Networks Forms of Organization (Adapted from Research in Organizational Behaviour 12 (1990, pp. 295–336),' in G. Thompson, J. Frances, R. Levacic and J. Mitchell (eds.), *Markets, Hierarchies & Networks: The Coordination of Social Life* (London: SAGE Publications).
- Rasmussen, J. (1982), 'Human Errors. A Taxonomy for Describing Human Malfunction in Industrial Installations,' *Journal of Occupational Accidents*, Vol. 4, pp. 311–33.
- (1983), 'Skills, Rules, and Knowledge; Signals, Signs, and Symbols, and Other Distinctions in Human Performance Models,' *IEEE Transactions on Systems, Man, and Cybernetics*, SMC-13, pp. 257–66.
- Reason, J. T. (1990), *Human Error* (Oxford: Oxford University Press).
- (1997), *Managing the Risks of Organizational Accidents* (Aldershot: Ashgate).
- Reid, J. and K. Catchpole (2011), 'Patient Safety: A Core Value of Nursing – So why is Achieving it so Difficult?' *Journal of Research in Nursing*, Vol. 16, pp. 209–23.

- Rodan, S. and C. Galunic (2004), 'More than Network Structure: How Knowledge Heterogeneity Influences Managerial Performance and Innovativeness,' *Strategic Management Journal*, Vol. 26, pp. 541–62.
- Royal Society (1983), *Risk Assessment: A Study Group Report* (London: Royal Society).
- (1992), *Risk: Analysis, Perception and Management* (London: Royal Society).
- Seidl, D. (2007), 'The Dark Side of Knowledge,' *Emergence: Complexity and Organization*, Vol. 9, pp. 16–29.
- Sipika, C. and D. Smith (1993), 'From Disaster to Crisis: The Failed Turnaround of Pan American Airlines,' *Journal of Contingencies and Crisis Management*, Vol. 1, pp. 138–51.
- Smith, D. (1990), 'Corporate Power and the Politics of Uncertainty: Risk Management at the Canvey Island Complex,' *Industrial Crisis Quarterly*, Vol. 4, pp. 1–26.
- (2000), 'Crisis Management Teams: Issues in the Management of Operational Crises,' *Risk Management: An International Journal*, Vol. 2, pp. 61–78.
- (2004), 'For Whom the Bell Tolls: Imagining Accidents and the Development of Crisis Simulation in Organisations,' *Simulation and Gaming*, Vol. 35, pp. 347–62.
- (2005a), 'Dancing Around the Mysterious Forces of Chaos: Exploring Issues of Complexity, Knowledge and the Management of Uncertainty,' *Clinician in Management*, Vol. 13, pp. 115–23.
- (2005b), 'Business (not) as Usual – Crisis Management, Service Interruption and the Vulnerability of Organisations,' *Journal of Services Marketing*, Vol. 19, pp. 309–20.
- and A. Irwin (2006), 'Complexity, Risk and Emergence: Elements of a "Management" Dilemma,' *Risk Management: An International Journal*, Vol. 8, pp. 221–6.
- Taylor, D.E. (2000), 'The Rise of the Environmental Justice Paradigm. Injustice Framing and the Social Construction of Environmental Discourses,' *American Behavioral Scientist*, Vol. 43, pp. 508–80.
- Templeton, S.-K. and J. Follain (2012), 'Leak Rate of Faulty Implants is 1 in 3 in the UK,' *The Sunday Times* (8 January, p. 12).
- Thomson, H. (2013), 'What's on Your Plate?' *New Scientist*, Vol. 217, pp. 6–7.
- Turner, B. A. (1976), 'The Organizational and Interorganizational Development of Disasters,' *Administrative Science Quarterly*, Vol. 21, pp. 378–97.
- (1978), *Man-Made Disasters* (London: Wykeham).
- Weick, K. E. (2001), *Making Sense of the Organization* (Oxford: Blackwell).
- and K. M. Sutcliffe (2001), *Managing the Unexpected. Assuring High Performance in an Age of Complexity* (San Francisco, CA: Jossey-Bass).
- Williams, R. (2013), 'Asda Clears Shelves of Value Burgers as Horsemeat Scandal Knocks £300m off Tesco Market Value,' *The Independent* (16 January) (Accessed on line at 1937 hours on 11 February, 2013).