Fischbacher-Smith, D. (2017) When organisational effectiveness fails: business continuity management and the paradox of performance. *Journal of Organizational Effectiveness: People and Performance*, 4(1), pp. 89-107. (doi:[10.1108/JOEPP-01-2017-0002](https://doi.org/10.1108/JOEPP-01-2017-0002))

This is the author's final accepted version.

There may be differences between this version and the published version. You are advised to consult the publisher's version if you wish to cite from it.

<http://eprints.gla.ac.uk/135454/>

Deposited on: 27 January 2017

When organisational effectiveness fails: business continuity management and the paradox of performance

Introduction

“Complexity is a defining characteristic of society and many of its technologies today. Yet simplicity and linearity remain the defining characteristics of the theories we use to explain bad events that emerge from this complexity” – (Dekker, 2011) p. 6.

The management of organisational performance demands the attention of many stakeholders within organisations and across both public and private sector organisations. As this Journal and others demonstrate, academic research on performance reflects both the variety and the multi-disciplinary nature of the issues around measuring and managing performance. Failures in organisational performance have also invariably attracted considerable attention due to the nature of a range of disruptive events. High profile failures, ranging from catastrophic technical or service failures (recent examples include the failure of the London Ambulance Service computer system and the hacking attack on *TalkTalk*) through to the collapse of a number of financial institutions in the 2008 banking crisis and the associated reputational failures, have been evaluated from a similarly broad, multi-disciplinary set of perspectives. The multi-disciplinary crisis management literature seeks to speak to the causal factors for such catastrophic events, as well as evaluating the task demands associated with the operational crisis and the post-crisis recovery period (Pearson & Clair, 1998; Smith, 1990, 1995). Much of that literature recognises the complexity referred to by Dekker in the opening quote and non-linear

behaviour within socio-technical systems is seen as a key element in shaping the ways that crises emerge. Management practice – a key focus of this paper – typically addresses failures within systems in terms of poor organisational performance and effectiveness. Organisations seek to mitigate these risks by developing Business Continuity Management (BCM)¹ plans to allow managers to cope with the task demands of a crisis. BCM as a significant form of management practice, advocates that organisations should identify key strategic vulnerabilities, priorities, and their associated underpinning systems, processes and data, and ensure that the organisation has plans in place to manage, preserve and, in the event of a crisis, recover so that the business can continue without disruption (or with minimal disruption) (see, Mcilwee, 2013).

As a management practice, BCM lays claim to be a holistic process that deals with a range of task demands generated by disturbances across the range of activities undertaken by the organisation. The extent to which these BCM plans are effective also becomes part of the wider assessment of organisational performance and hence creates a potential paradox within organisations. BCM plans are often assumed to be able to deal with the task demands of failure, and yet they do so under a management culture that may have led to the failure in the first case. BCM also lays claims to be holistic in its scope – both in terms of its coverage across organisational functions and, by inference, across the range of disciplines that comprise ‘management’ within organisational settings. There is also a paradox in that BCM could also be seen to be based on the rational,

¹ For the purposes of our present discussion, crisis management is seen as a broad-based process that deals with the pre- and post-crisis phases as well as the operational crisis. BCM is seen here as a more narrowly defined activity that is incorporated within crisis management. However, it should be noted that considerable debate exists around the exact meaning of the terms, especially as they relate to each other.

positivistic approach to management - that basically assumes that if you can measure it you can manage it – and yet it is seeking to deal with the demands generated by non-linear systems in a largely linear way.

In reality, the practice of BCM can be seen to be somewhat narrower in its scope and may fail to fully address the holistic, complex and non-linear nature of organisational performance and failure. Despite this, its adoption and dissemination amongst the growing body of BCM practitioners and the emergent professional infrastructure that surrounds it would suggest that can offer more to organisations than it currently does at present. If BCM could achieve its goal of being holistic in scope, then it would be in a position to change many of the command-and-control assumptions that exist across an organisation. At present, BCM, and to an extent the broader theories of crisis management, do not have a large-scale presence within business education and there are few specialised degrees in the area that would allow for the development of an appropriate skills set amongst managers (Fischbacher-Smith & Fischbacher-Smith, 2013, 2016). A first step in developing BCM as a core academic discipline within business education would require agreement about the parameters of the key terms used within the discipline and the development of a robust research agenda that strengthens the theoretical underpinnings of the subject.

The aim of this paper is to consider how BCM is defined within the professional and academic communities that work in the area. As part of this assessment, the paper will set out the key elements that emerge from the definitions of BCM and consider how the various elements of BCM can interact with each other in the context of organisational performance. Of particular

concern here, is the manner in which vulnerabilities are embedded within organisational processes – a process described by Turner as ‘incubation’ – and this applies to the development of BCM strategies as well as the overall strategic direction of the organisation. The paper deals primarily with the complexities associated with managing these disturbances and the role that incubation can play in the various dimensions of BCM as a process. By way of illustration, the paper draws on the *Talk Talk* case to illustrate the challenges of BCM in practice.

Although retaining a primary focus on the practice of BCM, the paper continually draws on the surrounding literatures on crisis management, safety, and security that provide additional insights into organisational responses to disturbances. The paper concludes by pointing to a range of considerations for academic research around the performance of BCM and the significance of recent work on crisis and safety science failure within that wider setting. The starting point for this discussion is with the nature of the BCM process itself. The paper examines some of the key definitions of BCM in order to set out the main elements of the term. It then considers the challenges for BCM arising out of the *TalkTalk* hacking case before exploring the interactions between success and failure.

Wither business continuity management? The search for meaning.

The meanings given to key organisational constructs are important elements in the development of a shared understanding of the practicalities of the entity being described. These definitions impart meaning and also help in the development of processes around understanding and communication of BCM

issues within organisations. The issue of definition is not simply about the words used, but what is meant by the “underlying concepts” (Perneger, 2006). This is particularly important when those concepts are multi-dimensional and multi-layered. These definitions are important in helping us to provide meaning and efficient shortcuts – definitional schema if you like - that allow us to make sense of the often abstracted mental structures that we hold about the world (Bartlett, 1932). These schema are particularly important within the complex setting of organisations and especially when dealing with issues that are at the margins of our experience and understanding, such as those found under conditions of crisis.

There are a range of definitions of BCM that are provided by both the academic and practitioner communities and which help set the parameters of the term and its practice-based limits. Ideally, these definitions should remove any ambiguities around the practicalities that might exist of what BCM means for managers in organisations and should serve to help frame the parameters of the relationships between BCM and other aspects of organisational performance.

The starting point for this discussion is with the British Standards Institution, which defines BCM by looking at it through the lens of the resilience construct (itself a potentially ambiguous term). It and frames BCM as:

“the ability of an organization to anticipate, prepare for, respond and adapt to incremental change and sudden disruptions in order to survive and prosper. It reaches beyond risk management towards a more holistic view of business health and success. A resilient organization is one that

not merely survives over the long term, but also flourishes - passing the test of time.” (British Standards Institution, 2016)²

The key elements of this definition relate to the anticipation of disruptive events and the holistic approach that is taken to the preparation and implementation of strategies to deal with the threats that have been identified. It is not clear, for example, whether these disruptions include catastrophic events or low-probability, high consequence hazards (often termed extreme events). The scale of any disruptive event can impact on an organisation’s absorptive capacity to deal with the task demands that it generates. Disruptions can be generated by both internal or external factors, both of which can expose pre-existing vulnerabilities within the organisation. The definition also sets out the relationships between these disruptions - it is worth noting that the term crisis is not used here - and the success of the organisation. In some respects, this definition of BCM has much in common with the literatures relating to organisational agility and the development of dynamic capabilities, especially as they relate to processes around knowledge management (see, for example, Aitken, Christopher, & Towill, 2002; Becker, 2001; Teece & Pisano, 1994; Teece, Pisano, & Shuen, 1997). Resilience, which is seen as a key component of the process, is framed in terms of ongoing business success and longevity and so the temporal dimensions of BCM are incorporated into this definition. The definition does not see these disruptive events as being simply catastrophic but suggests that they may arise from a range of threats that may be sudden or incremental in their onset.

² <http://www.bsigroup.com/en-GB/our-services/Organizational-Resilience/>

One of the striking elements of this definition is that it sees BCM as moving beyond conventional approaches to risk management towards a more holistic approach to the management of performance. An assumption here could be that risk management – with its emphasis on the aggregation of the risks of component failures, the focus on a priori evidence, and the determination of probabilities and consequences – may not be capable of dealing with issues in a holistic manner or with emergent forms of hazard. It may also prove problematic in those situations where the probabilities and consequences of an event are uncertain or indeterminate. However, these constraints could also be seen to apply to business continuity approaches, especially given the diverse range of threats that an organisation may face. A second argument could be made that much organisational risk management activity is seen as being focussed on operational, rather than strategic, issues, although the growth in work around enterprise risk management (ERM) could be seen to contrast with such a criticism. (Beasley, Clune, & Hermanson, 2005; Gordon, Loeb, & Tseng, 2009; O'Donnell, 2005). Whilst in theory, there is considerable potential for overlap between the processes of BCM and enterprise risk management, the focus within ERM on the processes of audit and accounting has led some to argue that it is too narrow a construct, and that the more holistic approach, such as that claimed within BCM, may prove to be preferable. Power, for example, argues that:

“in the quirky and evolving world of BCM practice there is a nascent recognition that security is only possible as a collective activity. While this is far from being unproblematic, it contrasts with ERM, where we now know that security is at best limited to certain states of the world and at worst is illusory” - (Power, 2009), p.853.

This is dependent, of course, on BCM being able to develop the holistic and coherent approach to managing and responding to the risk matrix facing the organisation that it seeks to achieve.

Much of the concern with ERM is around its focus on the auditable nature of the process. This could be seen as encouraging a more reductionist approach to identifying and managing threats rather than framing them in a more holistic way. Another issue here relates to the empirically-based nature of many risk assessment processes which do not easily lend themselves to dealing with those emergent forms of hazard for which there is no previous experience or for the actions of individuals who seek to cause harm. In these cases, the lack of a priori data about the threats could be seen to be a potentially inhibiting factor in terms of raising awareness of vulnerabilities. An approach that looks at vulnerabilities as well as threats, will require the development of an extensive knowledge-base in order to achieve this holistic approach. Power also highlights the importance of the knowledge base that underpins both ERM and BCM. This is a point that will be returned to later as it may prove to be a significant weakness in the current configuration of BCM in practice.

Other definitions of BCM from the perspective of the professional bodies provide additional boundaries to the parameters of BCM. The UK's Business Continuity Institute (BCI), for example, also defines BCM by reference to resilience and sees the process as being:

“.....about building and improving resilience in your business; it's about identifying your key products and services and the most urgent activities that underpin them and then, once that 'analysis' is complete, it is about

devising plans and strategies that will enable you to continue your business operations and enable you to recover quickly and effectively from any type disruption [*sic*] whatever its size or cause. It gives you a solid framework to lean on in times of crisis and provides stability and security”. – (Business Continuity Institute)³

Again, the key issue here is what is meant by resilience, as it can also been seen as an ambiguous term due to its development across different academic disciplines (Haimes, 2009; Hawley & DeHaan, 1996; Holling, 1973; Holling & Gunderson, 2002).

Another key premise within the BCI definition relates to the development of a “solid framework to lean on in times of crisis” (op cit). Again there is potential for ambiguity here as it does not indicate whether that framework addresses all of the phases of a crisis (that is, pre-, post, and operational). The BCI definition also sees an effective plan as being able to deal with the task demands of a crisis irrespective of its scale. As scale, expressed in terms of consequences, is seen as a key element in shaping the capability of organisations to manage a crisis, then this scale-free proposition is a particularly challenging one. Other definitions, as we will see, do suggest that scale is a factor in determining the performance of BCM.

These issues highlight questions about the range of skills that would be required by BCM professionals in order to work at the holistic levels that the various definitions see as key to the process. An important issue here is the way that BCM managers are trained and how this allows them to develop the skills

³ <http://www.thebci.org/index.php/resources/what-is-business-continuity>

and capabilities needed to work across the organisation in a holistic manner. This discussion, whilst central to the issue of organisational performance, is outside of the scope of our present discussions, but is clearly an area where further discussion is needed in this journal.

Moving away from a UK perspective, the US-based Disaster Recovery Institute has also sought to address the definitional issues by bringing together a number of the key terms used in an attempt to standardise the language used (DRI International, 2016). Within this context, they have adopted the definition of BCM that is used within the ISO standard 22301 in which BCM is seen as a:

“Holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities” – (DRI International, 2016)

The DRI goes on to provide further elaboration on the definition of BCM which strengthens further the link with resilience as a key element of the construct. Here BCM is seen as:

“a management process that identifies risk, threats and vulnerabilities that could impact an entity's continued operations and provides a framework for building organizational resilience and the capability for an effective response. The objective of Business Continuity Management is to make the entity more resilient to potential threats and allow the entity to

resume or continue operations under adverse or abnormal conditions. This is accomplished by the introduction of appropriate resilience strategies to reduce the likelihood and impact of a threat and the development of plans to respond and recover from threats that cannot be controlled or mitigated” – (DRI International) ⁴.

Although resilience forms a key part of these definitions of BCM, it is not clear which of the various perspectives on the resilience construct is seen to underpin the development of these strategies around BCM. The DRI Glossary defines resilience as: “the adaptive capacity of an organization in a complex and challenging environment” (p. 24) and qualifies this by reference to the ASIS/BSI standard in which the term is used to describe the organisation’s abilities to deal with the task demands of a disruption or return to an acceptable operational state within an appropriate time period. Again by reference to ASIS, the glossary defines resilience as:

“the capacity of a system to maintain its functions and structure in the face of internal and external change and to degrade gracefully when it must” (p. 24).

This approach could be seen to have much in common with the engineering approaches to resilience, in which the defining characteristic is the ability of the entity to return to its prior equilibrium state after a disturbance. In some respects, these definitions of BCM might be seen to have introduced more ambiguity into the meaning of business continuity through its use of resilience as an underlying element of the definition. Some of the apparent contradictions

⁴ <https://www.drii.org/certification/professionalprac.php?lang=EN>

within the definitions also add to this sense of greater ambiguity. On the one hand, some of the definitions see BCM as going beyond normal approaches to risk management (for example, the BSI definition) whilst others have a focus on the assessment of risk in what appears to be a fairly conventional way.

Academic definitions of BCM also emphasise different elements of the process. An entry in the *Encyclopaedia of Crisis Management*, for example, sees BCM as “emergency planning for business” (p. 74). This introduces yet another concept, that of emergency, which has also proved to be difficult to define and is often framed within catastrophic events that usually involve mass casualties and which are managed by government agencies (Gross, 2008). In the Mcilwee definition, these events appear to be excluded from the BCM definition if they involve natural disasters that are so large as to require government involvement in the recovery period. The definition also seems to exclude those disturbances that result from a failure in governance aimed at protecting the organisation (Mcilwee, 2013). Exclusions such as these do little to add clarity to the parameters within which BCM operates. In terms of the practices that BCM undertakes, Mcilwee does provide greater clarity by setting out the concept of the BCM wheel that envisages six core steps in the development and maintenance of an effective BCM process (see Figure 1).

Figure 1 - the BCM wheel

SOURCE: Based on Mcilwee (2013)

The starting point here is with the programme management of BCM which is seen by Mcilwee as being an extension of project management (another functional discipline within the management area). Ideally, BCM should be overseen by a steering group that draws on the range of functional expertise that exists within the organisation (Mcilwee, 2013). However, Mcilwee does make an exception to that inclusive process. For some reason, he sees IT disaster recovery as being outside of the BCM process as it is considered to be a normal aspect of the IT function. Given the claims that BCM is a holistic process and given the centrality of information technologies in modern organisations, then such an omission seems to be somewhat contradictory. The determination of the scope of the BCM process is the second stage of the wheel. If key functional areas are omitted from any business impact analysis then it will inevitably constrain the development of the understanding process. Subsequent stages in the

development of the BCM strategy will invariably be inhibited by any gaps or weaknesses in the knowledge base that underpins the assessment of the threats and vulnerabilities facing the organisation. A robust business impact analysis can be seen to form part of an organisation's protective structures but a partial assessment can serve to generate additional vulnerabilities. These protective structures are designed to help prevent complex systems from failing and are inevitably shaped by issues around knowledge management and information flows that affect the performance of relationships between functions and these protective structures (Dekker, 2011). The consequence is that the protective mechanisms put in place within the organisation, of which BCM could be seen as a key component, may themselves help to cause harm if they are based upon a set of flawed assumptions and information constraints. Notions of organisational limits are also important here in terms of shaping performance. The focus on component failures in traditional approaches to dealing with hazards has been seen to ignore the connectivities and interdependencies that exist between those components (Leveson et al., 2005; Roberts, Madsen, & Desai, 2005). This would also apply to the interactions between the components of the BCM process shown in figure 1. We have already alluded to the problems associated with excluding some functional areas from the BCM programme, as this will impact on the understanding of the threats that the organisation faces as well as the performance of key functional areas and their interactions with other parts of the organisation. Any weakness in the early stages of the BCM wheel will inevitably impact on the subsequent stages, thereby incubating the potential for failure into the very protective structures that are designed to prevent such failures from occurring.

The holistic nature of the BCM process is also addressed in the definition provided by Hebane et al, who state that:

“...business continuity management (BCM) has evolved into a process that identifies an organisation’s exposure to internal and external threats and synthesises hard and soft assets to provide effective prevention and recovery. Essential to the success of BCM is a thorough understanding of the wide range of threats (internal and external) and a recognition that an effective response will be determined by employees’ behaviour during the business recovery process” - (Herbane, Elliott, & Swartz, 2004), pp. 435-436.

There are several key elements of this description of BCM that are relevant to the discussion of organisational effectiveness. Firstly, there needs to be an effective process that addresses the *identification of the threat matrix* facing the organisation and, in an increasingly globalised environment, this needs to be carried out across the range of the company’s activities. These threats can arise from both *internal and external sources* and there may also be synergies between the various threat components that increases both the probability of failure and the consequences associated with it. This requires that those responsible for BCM develop an effective knowledge management programme that takes a wide perspective on organisation performance. Thus, knowledge management is a core activity that should be incorporated into the BCM wheel and should operate across the various elements in an explicit way.

Secondly, any intervention processes and plans that are designed to prevent or mitigate potential threats also need to ensure that they do not

escalate the problem still further. Intervention strategies need to consider the connections between the functional elements of the system and should also reflect BCM's role as part of the regulatory structures of the organisation. Ultimately, a failure in the project management process for BCM has the potential to incubate vulnerabilities into the organisation and move it into a state of crisis. The result is that the more complex the system is, the more the interactions between systems elements have the potential to generate emergent conditions which can lead to failure, despite each of the components working as designed (Hollnagel, 2012, 2014; Leveson, 2011; Perrow, 1984).

Thirdly, both *tangible and intangible assets* need to be deployed within the BCM wheel to deal with the task demands generated by a disruptive event. The tangible assets may require the provision of new premises, alternative supply chain relationships, key infrastructural components, and critical human resources, all of which are expensive and difficult to source during a crisis event. The availability of key tangible assets required to deal with a potential crisis will impact upon organisational effectiveness and the planning for them will entail considerable cost, especially for an event that might not occur. The issues of effectiveness and efficiency are placed in a symbiotic relationship at the core of the business continuity process. Greater efficiencies may, ultimately, erode organisational effectiveness, especially when dealing with low-probability, high-consequence events due to the cost of providing effective contingency arrangements for low-probability events. These extreme events highlight the challenge facing BCM in terms of the trade-offs that organisations make when planning for such hazards. On the one hand, the perceived view is that these are rare events and this has to be balanced against the potential harm that they may

generate if they do occur. Denying that such rare events can happen has been likened to a “Titanic syndrome” (Smith, 1993, 1995) in which the complacency generated by the event’s perceived low probability of occurrence serves to shape the conditions that ultimately allow the failure to occur.

The effectiveness-efficiency paradox becomes even more problematic when considering the intangible assets that are involved in the BCM process. These intangible assets can include such attributes as trust, reputation, perceived capability, informal networks, and intellectual property. Any effective BCM process needs to map and develop protective strategies for these attributes as part of a robust strategic process and has to deal with the causes as well as the symptoms of organisational failure. It is important to note however, that these attributes may also be damaged by an ineffective BCM process and this may, in turn, serve to escalate the overall harm associated with the event.

Finally, there is a clear view in the quote from Herbane et al that highlights the dependence of BCM on the performance of a range of actors within the organisation. The performance of these individuals and groups will be a function of the skills and attributes that have been developed to deal with the task requirements facing the organisation. These will include those tasks that exist in the organisation’s steady-state environment as well as those that lie outside of this designed-for state and will include a range of events that have the potential to generate a crisis. There is also an inherent paradox here as well. Why should we expect those managers who led the organisation into crisis to have the necessary skills and capabilities that are necessary to manage the organisation out of that crisis (Smith, 1990, 2000)? If we see a crisis as a set of exceptional

events, then there is an argument that it needs exceptional skills and capabilities to manage it. If, on the other hand, we see a crisis as arising out of the normal operating conditions within the organisation, then it raises a different set of challenges for organisations around the capabilities of all actors working within the wider system. It is in this context that the notion of dynamic capabilities (Teece & Pisano, 1994; Teece et al., 1997) can be seen to be important within the wider crisis management process. Whether BCM processes, as they are currently configured, provide these capabilities is a matter of some debate and the example of the TalkTalk hacking in 2015 serves to provide a brief illustration of some of the challenges associated with the task demands and practices of BCM.

It's good to talk – the TalkTalk crisis

TalkTalk was attacked by hackers on the 21st October 2015 and this was the third security breach that the company had experienced during that year (Bisson, 2015). The company initially described the magnitude of the attack as involving elements of the personal data of up to 1.2 million of their customers and this material may have included some 21,000 bank account details (BBC News, 2015c). This figure was later revised down to 150,959 customers, including the bank account details of 15,656 customers (BBC News, 2015b). The confusion around the extent of the data breach was also matched by the apparent confusion within the company's senior management team. During the crisis, the Chief Executive – Dido Harding – admitted on the BBC's Today programme that she did not know the full extent of the problem and the company had therefore taken the decision to warn its 4 million customers that

their data may be at risk (Saunders, 2016). Such an honest and open approach is unusual in many crisis situations but it could be seen as commendable and a rare admission that senior managers were not in control of the complex socio-technical systems that they operate. Such apparent confusion in the early stages of the crisis is not an unusual phenomena and neither was the high degree of media scrutiny associated with it. However, what was more unusual, was that the company seemed not to understand the technical nature of the attack, despite being a well-established internet company (The Register, 2015). The company also admitted that it had received a ransom demand from someone claiming to be the hacker (BBC News, 2015a). There was also some speculation, following claims of responsibility made online, that the hack could have been carried out by an Islamist hacking group (Khomami, 2015; Withnall, 2015), although this was later found not to be the case. For an IT company, issues around data security would be seen as quite fundamental to the nature of its core business and the confusion and ambiguity around the nature of the attack may have compounded the sense of crisis. The fact that it was later found that the hack was carried out by a 17 year old who admitted in court to “showing off” to his friends (BBC news, 2016; Heathman, 2016) only added to the sense of crisis and the limitations of the company’s security controls. The result was that:

“It quickly became apparent that neither Harding nor her fellow board members knew anything like as much as they should about the state of their data security – not only did they not know exactly what or how much data had been lost, or who had taken it, but there was even confusion over such basic questions as whether the lost details were encrypted” - (Saunders, 2016), p. 32.

The outcome of the company's response to the hack was that they were fined £400,000 by the UK's Information Commissioner's Office (ICO) due to the apparent ease by which the attack was perpetrated (Information Commissioner's Office, 2016). Media reports stated that this was the largest fine to-date for a data protection breach and cited industry insiders who observed that:

“the incident is only part of the story – the underlying breach is the failure to have appropriate measures in place. The hackers exploited a bug for which a fix existed. Not fixing a known problem is the definition of failing to put appropriate measures in place” – Tim Turner (2040 Training) (cited in Burgess, 2016a).

In addition to the fine, *TalkTalk* lost somewhere in the order of 95,000 customers and accrued losses of £60 million, made up of a £15 million trading impact and the rest as exceptional costs (Burgess, 2016b). Despite the costs of the hack, the company's overall revenue for the same quarter rose by 1.8% compared to the previous year (Burgess, 2016b). Dekker (2011) outlines a number of reasons why senior management may not have the level of control that is commonly perceived to exist. Firstly, uncertainty in a competitive and highly interconnected environment leads to local adaptations due to internal resource constraints as staff seek to achieve performance targets in a constrained context. Secondly, this drift away from an organisations designed-for-state takes place in small steps that go unnoticed and were the normalisation of deviations from established good practice can be made to 'get the job done'. Thirdly, the decisions taken at various points in the organisational life-cycle can impact on conditions further

down the time-line (termed error cost by Collingridge (1992)). Fourthly, the processes by which organisational activities are regulated can contribute to this incubation of failure potential (see, Dekker, 2011). It is likely that each of these elements identified by Dekker may have played a role in the *TalkTalk* crisis. The legacy issues around the software vulnerability that appear not to have been acted upon by the company highlights the importance of these elements and may also have contributed to the confusion within the company.

The *TalkTalk* attack illustrates the need for organisations to take a more holistic approach to BCM and one that incorporates the importance of the incubation processes identified by a number of authors (Collingridge, 1992; Dekker, 2011; Reason, 1997; Turner, 1976). It highlights the ways in which the potential for failure can be incubated as a result of routine operating processes including: the provision of information to senior managers about the risks that they face, the assumptions that they have around performance, the limitations of strength in-depth strategies, and the stove-piping that can take place between functional areas within the organisation (especially around security), and the impacts upon communication (Densham, 2015; McIntosh, 2015; Pace, 2016). The hack also highlights the role that such routine operational issues can have on the strategic performance of the organisation and their impacts on the generation of crisis.

Against the background of the *TalkTalk* crisis, there are issues around how BCM can deal with the pre-crisis incubation issues that served to compound the problem, and especially around the apparent lack of strategic engagement in identifying vulnerabilities. The vulnerabilities that were embedded within

TalkTalk's operating procedures were exposed by the hack but were not clearly created as a function of that external attack. They resulted from internal decisions and processes along with the presence of legacy issues within the decision time-line. The pre-crisis stage – termed a crisis of management (Smith, 1990, 1995) – allows for vulnerabilities to be embedded in organisational routines and they arose out of issues relating to systems design and the generation of emergent conditions that invariably exist within complex socio-technical systems. In addition, there are potential problems around the dominant mind-set that exists in organisations and which serves to shape the cultural paradigm through which decisions are taken (Fischbacher-Smith, 2012). This initial phase of a crisis is also typified by constraints around the flows of information which arise from both structural and cultural elements within the organisation and which shape and constrain the information around early warnings and weak signals (Ansoff, 1975, 1980; Fischbacher-Smith & Fischbacher-Smith, 2014).

If BCM and, perhaps to a more limited extent, crisis management, are not to be considered as the having a focus on the management of exceptions (Roux-Dufort, 2007, 2009), then it will need to overcome these challenges around the processes of incubation and actively seek to address the ways in which success and failure interact together to generate crisis events. This will require a skills-set that understands the holistic issues that face management and move away from a largely reactive approach to dealing with the threat matrix. In order to examine the nature of these challenges, it is first necessary to see how the various professional groupings that deal with BCM define the parameters of the term. The definition of terms used to shape organisational behaviours are an

important aspect of helping to frame the nature of performance as they provide a benchmark against which performance criteria can be judged. Ambiguities in those definitions or in the key parameters of process activities, may well impair performance.

Framing the parameters of business continuity

The range of BCM definitions outlined earlier showed that there is a lack of agreement about the ways that business continuity is framed. Whilst there are areas of commonality within the definitions, there are also some elements that are potentially contradictory. The example of the *TalkTalk* hacking crisis illustrated how challenging managing such an event can be, although it is not clear that all of the definitions would have agreed that this was an issue for BCM to deal with rather than the IT department. Many of the vulnerabilities within *TalkTalk* seem to have been embedded in the organisation prior to the event. The paper now seeks to bring together the key elements of BCM that emerge out of the definitions and to add additional elements that were highlighted in cognate literatures and from the *TalkTalk* case. Inevitably, this will not be a definitive exposition of the elements of BCM but, instead, is an attempt to highlight the common ground issues and those elements that need to be incorporated into the BCM agenda in order to allow it to achieve its holistic goals around hazard management.

One of the notable issues within all of the definitions of BCM relate to the key managerial process that are seen as being essential in allowing it to develop of a holistic approach. The specifics of these processes are not developed in

detail within the definitions but they are essential to the performance of BCM in practice. Figure 2 highlights the key elements drawn from these definitions, along with a number of additional elements that could be seen as important in supporting the BCM wheel. These include:

- The importance of ***emergent conditions*** in generating additional and unforeseen task demands for the organisation and which may allow events to exceed the limits of any contingency arrangements put in place within the organisation (Smith, 2000; Smith, 2005)
- The role played by ***extreme events*** in generating a unique set of circumstances for which the organisation has no contingency plans in place.
- ***Knowledge management*** and its dissemination,
- An understanding of the processes by which failures are *incubated* and how those processes relate to success,
- The development of ***dynamic capabilities*** amongst key actors in the system (Teece & Pisano, 1994; Teece et al., 1997),
- The provision of effective management training in order to overcome the challenges that are generated by a holistic approach. This would be a first step in avoiding the problems of weak management which has been seen as a factor in the generation of crisis (Turner, 1994). This is framed here within the context of the Chartered Management Institutes notion of the '***Accidental Manager***' syndrome – those individuals who hold managerial roles but without any formal training.

Figure 2 – Elements of BCM as practice

There are several challenges that arise out of the landscape of issues highlighted in Figure 2. The first of these relates to the skills requirements needed to work across the main elements incorporated into the definitions of BCM. By way of illustration, we can take the challenges presented by the ‘analytical diamond’ of issues that sits at the core of the threat matrix shown in Figure 2. Developing an understanding of the range of threats that an organisation faces is challenging in itself, but especially so considering the additional vulnerabilities that exist across the range of organisational processes and procedures in each of the functional areas. The skills needed to work across the portfolio of threats facing an organisation is considerable. To be effective,

those involved in BCM would need to have both managerial and technical competencies in order to deliver on the holistic claims set out in the definitions.

A second area where BCM might run into difficulties relates to the relationships with existing processes around risk management. The British Standards definition states that BCM can go beyond risk management by being more holistic – an argument that Power (2009) is also sympathetic to – but no indication is provided as to how BCM will adopt the strategic approach that would be needed to make this work or how it would ensure that business continuity issues are firmly placed on the board’s agenda. The DRI definition, on the other hand, sees BCM as a process that allows for the identification of “risks, threats and vulnerabilities” but this could be seen as falling within the existing remit of risk management approaches (including ERM), and it isn’t clear how BCM will differentiate itself from other cognate areas in this space.

Thirdly, each of the definitions makes reference to resilience as an outcome of the BCM process but none of the definitions acknowledge that resilience can also be a contested term. ‘Resilience’ has a range of different meanings across the main bodies of work that use the term and these include:

- *engineering*: where resilience is often framed in terms of the ability of the system to ‘bounce back’ from a shock event;
- *education and counselling*: where the importance of networks and support structures provides the necessary social relationships that are needed to deal with the task demands of a shock event;
- *systems biology*: where resilience is often framed in terms of the fitness of organisms (and organisations) to operate across different environmental

settings. In some respects, this has synergies with the notion of dynamic capabilities within an organisational setting.

So the notion of “building and improving resilience” referred to in the definition of BCM could well be seen as a fractured, if not a contested, space within which an understanding of the main elements of the term might prove to be difficult. For the purposes of our present discussions, the key elements here are the anticipatory and sustainability aspects of the resilience process. However, there is an argument to suggest that they are also key aspects of the main theoretical perspectives on crisis management.

Finally, there is the issue of defining the parameters of BCM. The DRI frames BCM as an umbrella term that has the potential to bring together and integrate the processes of: the *continuity* of organisational activities (through the relocation of activities after a disturbance), *disaster recovery* (framed in terms of IT recovery), *emergency response* (as the protection of life), and *crisis management* (expressed in terms of business protection)⁵. Each of these terms would, however, also be subject to definitional disputes that make the standardisation of terms problematic. For example, the term disaster has been explored in some detail within the academic literature (Quarantelli, 1978a, b, 1998a, b) and there is a view that sees a disaster as having a geo-physical core (Stallings, 2004), thereby excluding socio-technical systems. Within the computing area - a classic socio-technical system – a disaster is normally seen as relating to the failure of an IT system and the disaster recovery process is concerned with the response to a catastrophic failure of that system. So, despite

⁵ <https://www.drii.org/whatisbcm.php>

seeking to standardise the nature of definitions relating to BCM, some of the professional groupings that represent work in this area (and who also certify practitioners) are adding to the proliferation of 'definitions' without necessarily addressing some of the contradictions that exist within them. There are therefore some significant issues around the definitions used in practice to describe BCM, its relationships with other key activities and constructs (and their associated bodies of work), and the ways in which the definitions that are used can serve to shape practice.

The challenges here relate to the strategic requirements that an effective BCM process generates. Like corporate security, BCM is often not directly represented on the board of many organisations. The *TalkTalk* example highlights the problems that the lack of board awareness across both of these functional areas can generate. There is also the issue of the core skills that a BC manager would have relative to other senior officers within an organisation. Many of the board level functions are represented by well-established professional bodies – often with Chartered status – and many of these disciplines have a clear strategic focus. Areas such as management, marketing, finance and HRM are also all represented within the core curriculum of MBA programmes and each of them would claim to have a clear strategic focus. As such, they aim to provide a more holistic approach to dealing with the demands facing the organisation. At present, it is not clear that BCM is able to achieve this reach and significance within organisations and it is certainly not represented in the core curricula of business schools to the level that is required (Fischbacher-Smith & Fischbacher-Smith, 2013, 2016).

BCM should be seen as a multi-level process that has the potential to integrate both strategic and operational activities, is dependent upon tangible and intangible assets, and is a function of the skills, knowledge and capabilities that are held by actors within the organisation. All of these elements are dynamic and require adaptive responses in order to cope with an ever-changing treat environment that can impact upon organisational performance across space and time. There is also a synergy between the attributes and process of an organisation operating in a steady-state environment and which may impact upon performance as the environment changes. Turner (1976, 1978) framed these processes as akin to the incubation of a virus within the organisation in which the development of the problem remains undetected until its symptoms manifest themselves, often at the point of failure. The decisions and actions taken at various points in space and time, will impact (negatively or positively) on performance further down the timeline. An effective approach to BCM should seek to identify these early warnings and weak signals and do so from a strategic perspective.

If effectiveness and efficiency can interact together to determine organisational performance, then it follows that those interactions can have both positive and negative effects. These effects can impact both on the processes that generate the pre-conditions for crisis and may also inhibit the effectiveness of those business continuity processes that are designed to deal with that crisis should it occur. If, for example, an organisation is capable of incubating the potential for failure within its own processes and practices (Reason, 1990, 1997; Turner, 1976, 1978, 1994), then it may well also incubate the potential for failure within its contingency planning processes.

The boundaries between BCM and other functional areas within organisations are invariably fluid and multi-faceted. They are also dependent on the relationships that exist between the system-as-designed and its emergent state – that is, as a function of both the changes in the operating environment and the adaptations that are made to deal with these task demands. As a consequence, the distinction between success and failure within an organisation is often blurred, spatially and temporally constrained, and may be a function of the decisions taken over time that reflected a different set of task demands to those currently experienced. Inevitably, managers will have an incomplete understanding of the nature of these interactions and, as such, will struggle to understand the operating conditions of the system as it fluctuates and approaches its limits. If crisis management and BCM are to move beyond a situation where they are perceived as dealing with exceptional events, then it is necessary for the theories and practices associated with them to develop a more nuanced view about the relationships between success and failure.

If we frame failure – of which crisis is perhaps an extreme example – as an exceptional event then we fail to see how the routine, ‘normal’ ways of working within organisations generate the pre-conditions for failure. The practice of business continuity management should sit at the core of many of the debates around organisational effectiveness and performance. It represents the symbiotic nature of success and failure and it highlights the problems that organisational cultures can generate in terms of the incubation of failure potential, both in terms of the routine activities of the organisation and the preparation of contingency plans for exceptional conditions. As it currently

stands, BCM needs to draw more on the theoretical perspective offered by crisis management research.

Crisis management can be seen to have a focus on the addressing the pre-conditions of a crisis as well as the operational stage of the event (Smith, 1990). The early work of Turner (1976, 1978, 1994), for example, highlighted the importance of assessing those processes by which the potential for failure could be incubated. This was built upon by Perrow (1984) in describing the generation of normal accidents and Reason through the construct of latent conditions (1990, 1997). If, as this and subsequent work suggests, that crisis management is not just concerned with the control of exceptional events (Roux-Dufort, 2009; Roux-Dufort & Lalonde, 2013) but also recognises the importance of day-to-day activities within the organisation (Hollnagel, 2014), then any effective crisis or BCM approach should be seen as a core element of the management of the organisation. Ultimately, this requires BCM to be an inherently strategic and holistic process that integrates together a number of key organisational processes around human resource management, knowledge management, organisational learning, communication, and strategy. This would require BCM training to be a part of the core management development of staff within the organisation, thereby integrating BCM into the operational and strategic fabric of the organisation. In order to achieve that goal, it will require changes in the ways that managers are trained (Fischbacher-Smith & Fischbacher-Smith, 2016) and would lead to crisis management being a core element of management programmes such as the MBA (Fischbacher-Smith & Fischbacher-Smith, 2013).

Conclusions

“Crisis management is perceived as the management of exceptional or out-of-the-ordinary situations, but it does very little to help theorize the functioning of organizations. One of the reasons why organization theorists have shown little interest in theorizing the concept of crisis is that this concept fosters paradoxical attitudes” - (Roux-Dufort, 2007), pp. 105-106.

The relationships between organisational performance and the generation of crises can be seen to be paradoxical at a number of ways. Firstly, as Dekker observes, we work in complex, non-linear settings and yet we often seek to manage that complexity with simplicity and linear thinking. This paradox has long been recognised within the academic literature on systems (Ashby, 1947; Ashby, 1964; de Raadt, 1987) but organisations appear content to persist in developing control mechanisms that assume linearity around cause and effect relationships. Secondly, we position notions of crisis and failure as opposite systems states from success and high performance. Recent work has suggested, however, that such a binary view is problematic and that success and failure are symbiotic in many respects (Dekker, 2011; Hollnagel, 2014; Leveson, 2004). Thirdly, we see crisis as an inhibitor of organisational performance when in many respects the search for performance, and the associated strategy of management by metric, may contribute to the incubation of crisis potential. Finally, there is often a gap between the perceptions that managers have about the way in which the system works (its designed for state) relative to the way that it functions in practice (its emergent state). The gap between these two

systems states is a function of shifts in the environment that have required changes in the system at the local level in order to maintain performance levels. These adaptations often go unrecorded and senior management are often unaware that such changes have taken place (Fischbacher-Smith & Fischbacher-Smith, 2014).

This paper has sought to consider the nature of the BCM process and frame it within the context of organisational effectiveness. Both the practice and research based literatures acknowledge that in order to be effective, BCM must adopt a holistic approach to dealing with the issues that face organisations. Unlike many other aspects of organisational activity, BCM as a process has its own redundancy as a core aim – that is, organisations hope never to have to deploy their BC strategies but if they do then they have to be effective. The increasing scale and complexity of organisations and the geographical scale over which they operate, have the potential to generate emergent conditions that will have the potential to generate crises. More recent work in the risk and safety fields has pointed to the fact that failures can occur even when there are no failures at the component level and that problems can be generated within the spaces of interaction between components that can move an organisation into an unstable state. This is the inherent paradox that sits at the core of the BCM process and its relationships with organisational performance. As long as BCM and crisis management are seen as issues of exception within the management process then the challenges around organisational failures will continue to be an issue for managers to address. As long as mainstream management research sees these issues as peripheral to organisational theory then the BCM area will be starved of theoretical insights into the ways in which complex systems fail. As a

consequence, the paradoxical nature of the relationships between organisational performance and crisis will continue.

Acknowledgement

The author wishes to acknowledge the comments made on an early version of this paper by Moira Fischbacher-Smith, Paul Sparrow, and David Evans. As is customary, all errors of omission and commission remain those of the author.

References

- Aitken, J., Christopher, M., & Towill, D. 2002. Understanding, Implementing and Exploiting Agility and Leanness. *International Journal of Logistics Research and Applications*, 5(1): 59-74.
- Ansoff, H. I. 1975. Managing Strategic Surprise by Response to Weak Signals. *California Management Review*, 18(2): 21-33.
- Ansoff, H. I. 1980. Strategic issue management. *Strategic Management Journal*, 1(2): 131-148.
- Ashby, W. R. 1947. Principles of the self-organizing dynamic system. *The Journal of general psychology*, 37(2): 125-128.
- Ashby, W. R. 1964. *An introduction to Cybernetics*. London: Methuen.
- Bartlett, F. C. 1932. *Remembering: A study in the experimental and social psychology*. Cambridge: Cambridge University Press.
- BBC News. 2015a. TalkTalk cyber-attack: Boss 'receives ransom email'. *BBC News UK*, 23rd October 2015(Accessed on line at <http://www.bbc.co.uk/news/uk-34615226> on the 30th December 2016 at 1708 hours).
- BBC News. 2015b. TalkTalk hack 'affected 157,000 customers'. *BBC News*, BBC News Business, 6th November 2015(Accessed on line at <http://www.bbc.co.uk/news/business-34743185> on 26th December 2016).
- BBC News. 2015c. TalkTalk reveals exact scale of website cyber-attack. *BBC News*, BBC News UK, 30th October 2015(Accessed on line at

<http://www.bbc.co.uk/news/uk-34675235> on 26th December 2016 at 1545 hours).

BBC news. 2016. Boy, 17, admits TalkTalk hacking offences. *BBC News UK*, Accessed on line at <http://www.bbc.co.uk/news/uk-37990246> on 26th December 2016 at 1751 hours.

Beasley, M. S., Clune, R., & Hermanson, D. R. 2005. Enterprise risk management: An empirical analysis of factors associated with the extent of implementation. *Journal of Accounting and Public Policy*, 24(6): 521-531.

Becker, F. 2001. Organisational agility and the knowledge infrastructure. *Journal of Corporate Real Estate*, 3(1): 28-37.

Bisson, D. 2015. TalkTalk investigates breach that might have exposed 4M customers' info. *The State of Security. Tripwire.com*, 23rd October 2015(Accessed on line at <https://www.tripwire.com/state-of-security/latest-security-news/talktalk-investigates-breach-that-might-have-exposed-4m-customers-info/> on the 30th December 2016 at 1800 hours).

Burgess, M. 2016a. TalkTalk fined £400,000 after 150,000 customers details were stolen in 2015. *Wired.co.uk*, 5th October 2016(Accessed on line at <http://www.wired.co.uk/article/talktalk-fine-hack-400000> on 26th December 2016 at 1928 hours).

Burgess, M. 2016b. TalkTalk hack toll: 100k customers and £60m. *Wired.co.uk*, 2nd February 2016(Accessed on line at

<http://www.wired.co.uk/article/talktalk-hack-customers-lost> on 26th December 2016 at 2026 hours).

Collingridge, D. 1992. *The management of scale: Big organizations, big decisions, big mistakes*. London: Routledge.

de Raadt, J. D. R. 1987. Ashby's law of requisite variety: an empirical study. *Cybernetics and Systems: An International Journal*, 18(6): 517-536.

Dekker, S. 2011. *Drift into failure. From hunting broken components to understanding complex systems*. Farnham: Ashgate.

Densham, B. 2015. Three cyber-security strategies to mitigate the impact of a data breach. *Network Security*, 2015(1): 5-8.

DRI International. 2016. *International Glossary for Resiliency* (15th May 2016 ed.): DRI International.

Fischbacher-Smith, D. 2012. Getting pandas to breed: Paradigm blindness and the policy space for risk prevention, mitigation and management. *Risk Management*, 14(3): 177-201.

Fischbacher-Smith, D., & Fischbacher-Smith, M. 2013. Tales of the Unexpected: Issues Around the Development of a Crisis Management Module for the MBA Program. *Journal of Management Education*, 37(1): 51-78.

Fischbacher-Smith, D., & Fischbacher-Smith, M. 2014. What Lies Beneath? The Role of Informal and Hidden Networks in the Management of Crises. *Financial Accountability & Management*, 30(3): 259-278.

- Fischbacher-Smith, D., & Fischbacher-Smith, M. 2016. Crisis management as a critical perspective. *Journal of Management Development*, 35(7): 930-940.
- Gordon, L. A., Loeb, M. P., & Tseng, C.-Y. 2009. Enterprise risk management and firm performance: A contingency perspective. *Journal of Accounting and Public Policy*, 28(4): 301-327.
- Gross, E. 2008. How to justify an emergency regime and preserve civil liberties in times of terrorism *South Carolina Journal of International Law and Business*, 5(1): 1-34.
- Haimes, Y. Y. 2009. On the Definition of Resilience in Systems. *Risk Analysis*, 29(4): 498-501.
- Hawley, D. R., & DeHaan, L. 1996. Toward a Definition of Family Resilience: Integrating Life-Span and Family Perspectives. *Family Process*, 35(3): 283-298.
- Heathman, A. 2016. 17-year old given rehabilitation order for 2015 TalkTalk hack. *Wired.co.uk*, 13th December 2016(Accessed on line at <http://www.wired.co.uk/article/17-year-old-boy-sentenced-talk-talk-hack> on 26th December 2016 at 2018 hours).
- Herbane, B., Elliott, D., & Swartz, E. M. 2004. Business Continuity Management: time for a strategic role? *Long Range Planning*, 37(5): 435-457.
- Holling, C. S. 1973. Resilience and Stability of Ecological Systems. *Annual Review of Ecology and Systematics*, 4: 1-23.

- Holling, C. S., & Gunderson, L. H. 2002. Resilience and adaptive cycles. In L. H. Gunderson, & C. S. Holling (Eds.), ***Panarchy. Understanding transformations in human and natural systems***: 25-62. Washington DC: Island Press.
- Hollnagel, E. 2012. ***FRAM, the functional resonance analysis method: modelling complex socio-technical systems***. Boca Raton, FL: CRC Press.
- Hollnagel, E. 2014. ***Safety-I and safety-II: the past and future of safety management***. Farnham: Ashgate Publishing, Ltd.
- Information Commissioner's Office. 2016. ***Data Protection Act 1998. Supervisory Powers of the Information Commissioner - Monetary Penalty Notice TalkTalk Telecom Group PLC***. Wilmslow, Cheshire ICO (accessed online at <https://ico.org.uk/action-weve-taken/enforcement/talktalk-telecom-group-plc-mpn/>).
- Khomami, N. 2015. TalkTalk cyber-attack: company unsure how many customers affected. ***The Guardian***, Friday 23rd October 2015 (Accessed on line at <https://www.theguardian.com/business/2015/oct/23/talktalk-cyber-attack-company-unsure-how-many-users-affected> on the 30th December 2015 at 1728 hours).
- Leveson, N. G. 2004. A new accident model for engineering safer systems. ***Safety Science***, 42(4): 237-270.
- Leveson, N. G. 2011. Applying systems thinking to analyze and learn from events. ***Safety Science***, 49(1): 55-64.

- Leveson, N. G., Cutcher-Gershenfeld, J., Carroll, J. S., Barrett, B., Brown, A., Dulac, N., & Marais, K. 2005. Systems approaches to safety: NASA and the Space Shuttle disasters. In W. H. Starbuck, & M. Farjoun (Eds.), ***Organization at the limit. Lessons from the Columbia Disaster***: 269-288. Malden, MA: Blackwell Publishing.
- McIlwee, P. 2013. Business continuity management. In K. B. Penuel, M. Statler, & R. Hagen (Eds.), ***Encyclopedia of Crisis Management***: 74-76. Thousand Oaks: SAGE Publications.
- McIntosh, C. 2015. Cyber-security: who will provide protection? ***Computer Fraud & Security***, 2015(12): 19-20.
- O'Donnell, E. 2005. Enterprise risk management: A systems-thinking framework for the event identification phase. ***International Journal of Accounting Information Systems***, 6(3): 177-195.
- Pace, C. 2016. Why HR and IT departments should talk talk. ***Strategic HR Review***, 15(3): 118-122.
- Pearson, C. M., & Clair, J. A. 1998. Reframing crisis management. ***Academy of Management Review***, 23(1): 59-76.
- Perneger, T. V. 2006. Borges on classification. ***International Journal for Quality in Health Care***, 18(4): 264-265.
- Perrow, C. 1984. ***Normal Accidents***. New York: Basic Books.
- Power, M. 2009. The risk management of nothing. ***Accounting, Organizations and Society***, 34(6-7): 849-855.

- Quarantelli, E. L. (Ed.). 1978a. ***Disasters - theory and research***. Beverly Hills, CA: SAGE.
- Quarantelli, E. L. 1978b. Some basic themes in Sociological studies of disaster. In E. L. Quarantelli (Ed.), ***Disasters - theory and research***: 1-14. Beverly Hills, CA: SAGE.
- Quarantelli, E. L. 1998a. Introduction. The basic question, its importance, and how it is addressed in this volume. In E. L. Quarantelli (Ed.), ***What is a disaster? Perspectives on the question.***: 1-7. London: Routledge.
- Quarantelli, E. L. (Ed.). 1998b. ***What is a disaster? Perspectives on the question***. London: Routledge.
- Reason, J. T. 1990. ***Human error***. Oxford: Oxford University Press.
- Reason, J. T. 1997. ***Managing the risks of organizational accidents***. Aldershot: Ashgate.
- Roberts, K. H., Madsen, P. M., & Desai, V. M. 2005. The space between in space transportation: A relational analysis of the failure of STS-107. In W. H. Starbuck, & M. Farjoun (Eds.), ***Organization at the limit. Lessons from the Columbia Disaster***: 81-97. Malden, MA: Blackwell Publishing Ltd.
- Roux-Dufort, C. 2007. Is Crisis Management (Only) a Management of Exceptions? ***Journal of Contingencies and Crisis Management***, 15(2): 105-114.
- Roux-Dufort, C. 2009. The Devil Lies in Details! How Crises Build up Within Organizations. ***Journal of Contingencies and Crisis Management***, 17(1): 4-11.

- Roux-Dufort, C., & Lalonde, C. 2013. Editorial: Exploring the Theoretical Foundations of Crisis Management. *Journal of Contingencies and Crisis Management*, 21(1): 1-3.
- Saunders, A. 2016. The MT Interview: Dido Harding. *Management Today*(September/October 2016): 32-37.
- Smith, D. 1990. Beyond contingency planning - Towards a model of crisis management. *Industrial Crisis Quarterly*, 4(4): 263-275.
- Smith, D. 1993. Exploring the myth: The sinking of the Titanic. *Industrial and Environmental Crisis Quarterly*, 8(3): 275-288.
- Smith, D. 1995. The Dark Side of Excellence: Managing Strategic Failures. In J. Thompson (Ed.), *Handbook of Strategic Management*: 161-191. London: Butterworth-Heinemann.
- Smith, D. 2000. Crisis Management Teams: Issues in the management of operational crises. *Risk Management: An International Journal*, 2(3): 61-78.
- Smith, D. 2005. Dancing with the mysterious forces of chaos: issues around complexity, knowledge and the management of uncertainty. *Clinician in Management*, 13(3/4): 115-123.
- Stallings, R. 2004. Disaster, crisis, collective stress, and mass deprivation. In E. L. Quarantelli, & R. Perry (Eds.), *What is a disaster*. New York: Xlbris.
- Teece, D., & Pisano, G. 1994. The dynamic capabilities of firms: an introduction. *Industrial and corporate change*, 3(3): 537-556.

Teece, D. J., Pisano, G., & Shuen, A. 1997. Dynamic capabilities and strategic management. *Strategic management journal*: 509-533.

The Register. 2015. Further confusion at TalkTalk claims it was hit by 'sequential attack' *The Register*, 26th October 2015(Accessed on line at http://www.theregister.co.uk/2015/10/26/talktalk_sequential_attack/ on the 30th December 2015 at 1714 hours).

Turner, B. A. 1976. The organizational and interorganizational development of disasters. *Administrative Science Quarterly*, 21: 378-397.

Turner, B. A. 1978. *Man-made disasters*. London: Wykeham.

Turner, B. A. 1994. The causes of disaster: Sloppy management. *British Journal of Management*, 5: 215-219.

Withnall, A. 2015. TalkTalk cyber attack" 'Russia-based Islamic jihadists' claim responsibility for hack. *The Independent*, Friday 23rd October 2015(Accessed on line at <http://www.independent.co.uk/news/uk/crime/talktalk-cyber-attack-russia-based-islamic-jihadists-claim-responsibility-for-hack-a6705366.html> on the 30th December 2016 at 1733 hours).

About the author

Denis Fischbacher-Smith is Professor of Risk and Resilience at the University of Glasgow and he has worked in the areas of risk and crisis management for over 30 years as both an academic and a practitioner. He holds a PhD from the University of Manchester in the area of risk assessment and a

DLitt from the University of Glasgow for his work on crisis management and business continuity. He is a Chartered Manager and a Chartered Fellow of the Chartered Institute of Personnel and Development.