The enemy has passed through the gate

Insider threats, the dark triad, and the challenges around security

Denis Fischbacher-Smith
Adam Smith Business School, University of Glasgow, UK

Abstract

Purpose – The purpose of this paper is to highlight the potential role that the so-called "toxic triangle" (Padilla *et al.*, 2007) can play in undermining the processes around effectiveness. It is the interaction between leaders, organisational members, and the environmental context in which those interactions occur that has the potential to generate dysfunctional behaviours and processes. The paper seeks to set out a set of issues that would seem to be worthy of further consideration within the Journal and which deal with the relationships between organisational effectiveness and the threats from insiders.

Design/methodology/approach – The paper adopts a systems approach to the threats from insiders and the manner in which it impacts on organisation effectiveness. The ultimate goal of the paper is to stimulate further debate and discussion around the issues.

Findings – The paper adds to the discussions around effectiveness by highlighting how senior managers can create the conditions in which failure can occur through the erosion of controls, poor decision making, and the creation of a culture that has the potential to generate failure. Within this setting, insiders can serve to trigger a series of failures by their actions and for which the controls in place are either ineffective or have been by-passed as a result of insider knowledge.

Research limitations/implications – The issues raised in this paper need to be tested empirically as a means of providing a clear evidence base in support of their relationships with the generation of organisational ineffectiveness.

Practical implications – The paper aims to raise awareness and stimulate thinking by practising managers around the role that the "toxic triangle" of issues can play in creating the conditions by which organisations can incubate the potential for crisis.

Originality/value – The paper seeks to bring together a disparate body of published work within the context of "organisational effectiveness" and sets out a series of dark characteristics that organisations need to consider if they are to avoid failure. The paper argues the case that effectiveness can be a fragile construct and that the mechanisms that generate failure also need to be actively considered when discussing what effectiveness means in practice.

Keywords Uncertainty, Organization effectiveness, Dysfunctional behaviours, Insider threats, The toxic triangle

Paper type Research paper

Introduction

> […] effectiveness is not a concept but a construct. A concept is an abstraction from observed events, the characteristics of which are either directly observable or easily measured […] constructs […]. are constructed from concepts at a lower level of abstraction. The problem is

Journal of Organizational Effectiveness: People and Performance
Vol. 2 No. 2, 2015
pp. 134-156
Emerald Group Publishing Limited
2051-6614
DOI 10.1108/JOEPP-03-2015-0010

> that no one seems to be sure which concepts […]. are to be included in the construct of effectiveness, or how they are to be related – (Quinn and Rohrbaugh, 1983, pp. 363-364).

Some 30 years after Quinn and Rohrbaugh highlighted the abstract nature of effectiveness, some might still question whether the construct has been developed sufficiently to provide answers to the questions that were outlined in their early paper. In particular, the question of which concepts make up the construct of effectiveness is still a key issue. The argument developed in this paper is that organisations need to consider some of the darker elements that shape organisational performance and accountability if they are to comprehensively understand the relationships between effectiveness and failure. Effectiveness is clearly a multi-layered issue: it transcends disciplinary and functional boundaries; it evolves over space and time; and it is often seen as an essentially perceptual process. In many cases, however, we only recognise effectiveness by its absence – that is, when organisations fail and especially when they fail in a catastrophic manner. It is invariably the case that at the point of failure, we judge the organisation to have been ineffective. However, this remains a generally binary view of the effectiveness construct when, in reality, it covers a spectrum of systems states. One only has to look at the ways in which politicians recast the boundaries of their policies to see how fluid that notion of effectiveness actually is.

The debates that invariably surround the success of the foreign policy of countries provides us with several examples of the ever-changing boundaries of effectiveness. The descent of Iraq into a civil war, the emergence of Islamic State as a potent terrorist force (and one that some might even refer to as an emergent nation state), and the increasingly globalised nature of terrorism, all point to the temporal dynamics of effectiveness, the replacement of one set of policy problems with another (often expressed as blowback; Bergen and Reynolds, 2005; Pena, 2002; Simpson, 1988), and the embedded nature of error cost and incubation in shaping organisational performance (Collingridge, 1984; Turner, 1976). These are complex policy problems around effectiveness that do not lend themselves to simple solutions. Ashby's (1958, 1962) Law of Requisite Variety highlights the need to manage variety in the system with sufficient variety in controls and there are lessons here for the ways in which organisations seek to achieve effectiveness. A starting point for dealing with such variety is to adopt more holistic and multi-disciplinary approaches to dealing with effectiveness.

Sparrow and Cooper (2014) have advocated a more multi-disciplinary approach towards dealing with the range of challenges facing organisational effectiveness. As a response to that challenge, this paper outlines elements of the darker side of organisational effectiveness by focusing on a range of issues that have the potential to move the organisation into a state of crisis and which also have the issues of people and performance at their core.

The first aim of this paper is to try and outline some of the relationships between risk and effectiveness. This is a potentially large agenda issue and so the focus here is on starting a set of debates around these issues and to do so in a manner that recognises the symbiotic nature of risk and effectiveness. A particular focus in this paper is on what has been termed the "toxic triangle" (Padilla *et al.*, 2007) in which leaders (and, by logical extension, senior managers) can create an environment in which the potential for crisis is generated, or where other organisational members can by-pass lax controls to create harm. It is the contention here that many crises within organisations are self-generated by those very people who are charged with making the organisation effective. In part, this arises from the ambiguous nature of effectiveness itself but also from the central role that is played by uncertainty within organisational decision making.

The second aim of this paper is to explore the darker side of organisational effectiveness and, in particular, to consider the role played by insider threats in the generation of failure. The paper grounds the discussion within the processes of effectiveness before examining the potential role played by "dark triad" personality factors (Jonason *et al.*, 2012, 2014; Paulhus and Williams, 2002) in shaping dysfunctional behaviours that can then lead to the erosion of effective organisations.

Framing effectiveness

Management's abilities to deal with uncertainty are critical to the ways in which effectiveness is framed. The greater the level of uncertainty within the environment, the greater the amount of variety will be required around organisational controls and information management systems in order to manage it. To an extent, organisational contingency plans reflect that process, but they are invariably constrained by the assumptions that managers make about the potential scenarios that they face. Uncertainty is also a key factor in managing the performance and behaviours of people within the organisation. The misbehaviours of staff will have an impact on effectiveness, as will the more "heroic" responses that are made by individuals to bring failing systems back under control (Ackroyd and Thompson, 1999; Reason, 2008). In both extremes of behaviour, uncertainty is a key factor in shaping the "local" dynamics of effectiveness at specific points in space and time. By responding to one set of challenges – either structural or human – organisations risk creating sensitivities to other forms of disturbance (Hodge and Coronado, 2007; Streatfield, 2001; Tenner, 1996; Tsoukas, 1999; Tsoukas and Chia, 2002). This particular dynamic also calls into question the role and nature of expert judgements in shaping decisions around effectiveness.

There are several additional issues that are raised in the paper by Quinn and Rohrbaugh (1983) that have resonance for present discussions within this Journal as well as within the broader Academy. They also questioned a range of processes around the temporal dynamic of effectiveness, the central role of values in determining the key parameters of effectiveness, and the manner in which changes in the perceptions of effectiveness over time need to be incorporated into any discussion of what the construct means in practice (see also Quinn and Cameron, 1983). These issues, and the relationships between them, are often nested, and changes in one of the parameters of effectiveness can have a significant impact on other elements. For example, the values held by organisational members will serve to shape both the decision-making and sense-making processes that operate around the management of both people and processes. Values and assumptions also shape the ways in which we frame and evaluate effectiveness and this impacts upon the manner in which we then structure organisational controls to allow that effectiveness to be achieved. Values often change over time and they also interact with the dominant cultural artefacts that have evolved within the organisation to create the conditions in which people work. Values also invariably play a central role in shaping how different organisational actors and external stakeholders perceive the nature of effectiveness at different points in time and space and also at the points of interaction with elements of the organisation and its wider network. Our experiences and worldviews serve to shape the ways in which we judge the effectiveness of our own actions, the processes through which those actions are enacted, and the (cognitive) frames that we use to shape (or curtail) the parameters of our decision making around the achievement of effectiveness. Thus, when we look at effectiveness through the context of the key people and processes that prevail at any point in space and time, we are only seeing a snapshot of a wider set of complex dynamics at work within the "system".

Figure 1 highlights some of the issues surrounding effectiveness. This is only a partial snapshot of the issues and is not meant to be inclusive of all of the elements of the construct. The emphasis within Figure 1 relates to the ways in which uncertainty interacts with knowledge, expertise, and culture to create a set of challenges to achieving and sustaining effectiveness. The ways in which an organisation accumulates, communicates, and implements its knowledge is also a key factor in shaping the performance of the wider system (Ditillo, 2004; Tsoukas, 1997; Tucker, 2014). The uncertainty that surrounds this process and the gaps that exist between the task demands and the control mechanisms, will serve to generate the potential for failure that will evolve over time and space and will be further shaped by the prevailing culture of the organisation. In essence, this Rubic's cube of effectiveness generates a fundamental challenge for organisations. A failure to adapt to changing task demands will create fractures in controls and any new innovations may well generate emergent conditions that by-pass existing controls. In both cases, effectiveness will be eroded, although it may remain hidden until a disturbance generates perturbations that expose these vulnerabilities (Tenner, 1996; Turner, 1976). Management actions remain at the core of this process – both in terms of their inactions around the forces of incubation as well as their direct actions in creating the root causes of failure (Reason, 1997; Turner, 1978, 1994).

Given the complex nature of effectiveness, it needs to be framed as a multi-level issue that requires analysis through multiple, multi-disciplinary lenses. As such, it requires us to consider how the construct is differentiated at different levels within the organisation and how the differences in the approaches towards it, at each of those levels and across locations, can generate fractures in control and governance (see e.g. Piattoni, 2009; Rousseau, 1985) and erode performance (Eichener, 1997; Scharpf, 1997; Vogel, 1997). The result is the creation of gaps in organisational controls that allow perturbations within the system to by-pass multiple layers of defences. Against such a background, risk and uncertainty are central components of the processes that shape effective organisations. By developing and articulating the nature of the various "logics" that shape both the "constraints and opportunities" (Engelen, 2001) open to organisations, it is possible to begin to outline a set of "dark" issues that have the potential to undermine effectiveness.

The darker logics of ineffectiveness

There are several issues that arise out of a discussion of the potentially negative aspects around effectiveness and some of these are highlighted in Figure 2. This is not meant to be a comprehensive list of organisational elements and processes, but rather an attempt to highlight some of the parameters of a research terrain that explores the

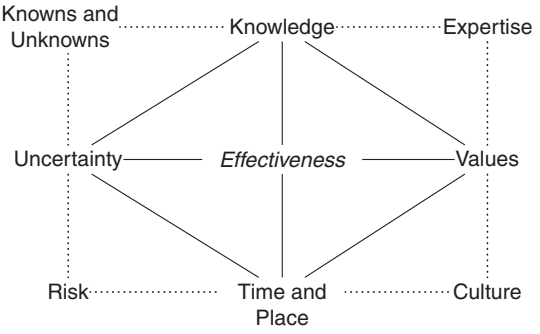


Figure 1. Framing effectiveness

Figure 2.
The terrain of (in)effectiveness

relationships between effectiveness and ineffectiveness (expressed here in terms of risk, crisis, and failure). At the core of these relationships are four issues that serve to shape the rest of the landscape.

The first of these relates to the processes around the management of people. The manner in which human resources can serve as either an enabler of effectiveness, or a key factor in undermining it, is a central element of the development of the wider logics of effectiveness. People within the organisation will help to create and shape the culture that prevails within it and, whilst this may be supportive of effectiveness, it may also be responsible for developing ways of working that prove to be corrosive and damaging (see e.g. Ackroyd and Thompson, 1999).

The second element relates to the ways in which the organisation functions as a holistic system. By focusing on elements of organisational processes, we invariably miss the subtle interactions between elements of the system that can ultimately bring about the conditions for failure. Our abilities to manage such emergent conditions also feeds back into the ways that we recruit, select, and train organisational members. This is especially problematic when working in a multi-national context. These extended organisational linkages operate across space, place, and time to generate a set of challenges around the effectiveness of organisational controls.

The impacts of space, place, time on organisational performance, along with the creation and maintenance of controls, constitute the third and fourth elements of the intellectual landscape over which effectiveness is ultimately to be framed. Space, place, and time increase the potential for emergent properties to generate conditions that lie outside of the "normal" parameters that are subject to organisational controls. This, in turn, creates conditions that challenge the worldviews of those who control the system and increases the task demands (especially around information provision), which then leads to impaired performance. This combination of new properties, problems around sense making, and the distributed nature of the organisation's employees can create further problems around control. The issues raised in Figure 2 represent a broad set of challenges that are raised by considering the opposite side of the effectiveness construct. Invariably, our present discussions will be focused on a limited set of these issues. The paper considers a particular "golden thread" of issues that have relevance

to the work on crisis incubation as outlined by Turner (1976, 1978), along with his framing of the management practices as part of this process (Turner, 1994).

The first of these relates to the role that people play in the crisis incubation process. By implication, this raises a challenge for the HR function around its abilities to address the processes of crisis incubation. In some respects, HRM could be seen as the neglected functional area within crisis management, despite the fact that it has the potential to shape the recruitment, selection and development of staff, the training of crisis management teams, and a range of activities around human resource development. The threats from insiders – both as the perpetrators of an "attack" on the organisation and as a point of vulnerability that can contribute to systems failure – should be a central issue of concern for the HR function. Instead, many organisations create an artificial boundary between the HR and corporate security functions. This Balkanisation of key activities has the potential to lead to the compartmentalisation of issues and creates barriers to effective flows of information, especially around early warnings of failure or misbehaviours. Ideally, the HR and security functions within organisations should reflect the symbiotic nature of their relationships when it comes to dealing with insider or outsider threats and misbehaviours. This would require the HR profession to ensure that personnel security is a more central component of its own activities and train HR professionals accordingly.

A second element arising from the issues raised in Figure 2 relates to the interaction between the HR function and the practices of the more "toxic" forms of management. This is due to the role of narcissistic and other dysfunctional behaviours within the management function and the role that these individuals can play in shaping organisational cultures, misbehaviours, and control mechanisms. Our discussion will turn later to highlight a range of concerns around the so-called "dark triad" of behavioural types (Jonason *et al.*, 2012; Paulhus and Williams, 2002) that have the clear potential to generate crisis conditions within organisations. The discussion will focus particular attention on the ways in which these behavioural issues have the potential to generate both violating- and error-producing conditions and, at the same time, allow for the erosion of organisational controls. Of particular importance here will be a consideration of the work of Reason in framing the processes associated with the creation of latent and active errors and violations in organisations (Reason, 1990a, b). Finally, the paper will consider the systems perspectives around the production of ineffectiveness, the role of negative innovation practices, the generation of emergent properties within systems, and the challenges facing organisations in terms of attempts to manage uncertainty.

The centrality of human resources

The first issue of note concerns the role of human resources in the management of performance and the potential it generates for crisis incubation. People are central to the ways in which the various logics of effectiveness are framed and implemented – both at an operational and a strategic level – but they also play a major role in the generation of ineffectiveness through exploitative and inadequate line management practices, poor decision making, insider threats, human error, and a range of managerial misbehaviours (see, amongst others, Ackroyd and Thompson, 1999; Burnett, 1998; Carmeli and Schaubroeck, 2006; Eriksson and McConnell, 2011; Pauchant and Mitroff, 1990; Woodford, 2012). For many organisations, the issues are framed around deviant behaviours without considering how organisational logistics and practices can contribute to dysfunctional behaviours. The projection of blame onto individual operators within a system invariably

masks the role that management, and a set of wider organisational processes, can play in shaping those behaviours by eroding organisational controls or by direct actions. One criticism that has been raised concerning the nature of misbehaviours and violations in the workplace is that managerial misbehaviours often go unpunished compared to lower level organisational members (Ackroyd and Thompson, 1999). A further factor here is the creation and sustaining of a set of flawed managerial assumptions around the way that the system functions in practice. The gap between these assumptions and the reality of the "system at work" has been a key factor in shaping organisational failures (Mitroff *et al.*, 1989; Pauchant and Mitroff, 1992; Reason, 1997; Turner, 1994).

The HR function can also play a significant role in helping to shape team and individual performance during a crisis (Smith, 2000) and in facilitating effective organisational learning in its aftermath (Smith and Elliott, 2007). Whilst there has been a considerable amount of research in the area of dynamic capabilities (Eisenhardt and Martin, 2000; Teece, 2014; Teece *et al.*, 1997; Winter, 2003) the application of those concepts to organisational crises – in terms of both causal and responsive processes – remains an under-researched phenomena. In particular, there is a need to understand how crisis-related capabilities are framed, what the main processes are around the development of those capabilities, and the implementation of the resulting capabilities frameworks within the context of crisis management teams. This process touches upon such issues as: knowledge management (and specifically, the capture and dissemination of tacit knowledge held by the individual that is critical to the performance of the organisation); the development of the dynamic capabilities required to both prevent and respond to crisis events; and the minimisation of threats from insiders (Smith, 2000, 2004; Snell and Youndt, 1995; Turner and Makhija, 2006). In some respects, the work on high-reliability organisations (LaPorte and Consolini, 1991; Roberts *et al.*, 1994; Sutcliffe, 2011) could be seen as offering considerable potential to extend the work on dynamic capabilities into the area of crisis management. Whilst high-reliability theory may be contested (Perrow, 2009; Sagan, 1993), it has been applied in a number of settings and there is some potential in exploring the implications of the approach within more general performance settings (Roberts *et al.*, 2001; Shrivastava *et al.*, 2009; Sutcliffe, 2011). Again, this is an area where HRM has a potentially significant role to play.

HRM should seek to play a more integrated "life-cycle" role in dealing with issues of effectiveness and performance through a focus on recruitment, selection, job design, staff development, security, and performance monitoring. A focus on the human aspects of reliability and the nature of a dynamic response to threats and vulnerabilities is key in this regard. In order to achieve this, HRM would need to deliver on its strategic promise around HR development (rather than maintaining a skewed focus on performance) and the practical implementation of "life-long" learning in achieving effectiveness. A key aspect of this process concerns the development of crisis management team capabilities and the associated training and exercising that is needed to support such processes. Again, this is a potentially important role for human resource professionals to add to organisational capabilities around effective performance. At present, this is not something that forms a significant part of HRM custom and practice and does not have the presence within the research community that it should. What work has been undertaken has pointed to the important role that HRM can play in the development of crisis preparedness (Sheaffer and Mano-Negrin, 2003) but, ultimately, HR will need to display its strengths as an enabler of organisational strategy and its abilities to help develop the capabilities that organisations need to both prevent and deal with the task demands of crisis.

This challenge also raises a core question about the effectiveness of the HR profession itself and its abilities to deliver on such a strategic agenda within organisations. Some commentators have gone so far as to suggest that the profession is in a state of crisis (Thompson, 2011), and this could be a significant factor in shaping the processes around organisational effectiveness. Thompson observes that:

> HRM is indeed in trouble, both theoretically and practically. Its core claims and professional self-image have become so entwined with the human capital narrative and the performance pot of gold at the end of the best practice rainbow for it to be any other way – (Thompson, 2011).

If HR has such a potentially fatal flaw within its own theoretical underpinnings then it is unlikely to be able to contribute to debates around effectiveness in any meaningful manner. There is, therefore, a clear dilemma for the HR community in the shareholder-driven culture that Thompson describes, where the focus on performance has resulted in the dominance of short termism within decision making and where the financial imperative has become the dominant measure of performance.

A core question here might centre on how HR contributes the expertise aimed at developing the dynamic capabilities that are needed within crisis management. This is especially problematic when the profession itself does not emphasise those processes in its own training and development programmes. A brief examination of accredited masters degree programmes in the UK illustrates that there is little coverage of risk and crisis issues facing organisations beyond tangential coverage in modules on ethical behaviours and industrial relations[1]. The one exception was the University of Strathclyde that offered an optional module in "The Psychology of Risk Management"[2]. There is an argument for increasing the centrality of HR in developing a crisis prepared culture within organisations and ensuring that is done in partnership with all employees and not just senior management. As if to reinforce the centrality of risk within HR, Thompson and colleagues have also observed that there is a strong relationship between HR practices and organisational controls (Ackroyd and Thompson, 1999; Thompson and van den Broek, 2010).

For such controls to be effective they need to be designed in such a way that they reflect our understanding of behaviours and the factors that shape them. These controls also have to be consistently tested and done in a way that challenges the assumptions that managers have about the ways in which those controls function. There is relatively little discussion within the general HR literature around these issues. Much of the discussion around insider threats, for example – and one might argue this is a key area of relevance to HRM – has been led by work emanating from within computer science and accounting (Berry *et al.*, 2009; Colwill, 2009; Kraemer and Carayon, 2007; Power and Forte, 2006) and by the Centre for the Protection of National Infrastructure in the UK. There are many instances where the controls have failed to prevent a trusted employee from causing harm, either by reputational damage, information theft, financial loss, or even by violent acts (Ambrose *et al.*, 2002; Bentley *et al.*, 2014; Brown, 2005; Day, 2007; Kramer and Heuer, 2007; Terry, 2013). Even the most "secure" organisations have proved to have problems in this regard and there are numerous examples of how even the security services and the military have failed to identify and act on insider threats, leading up to the more recent problems around Bradley Manning and Edward Snowden (Harding, 2014; Hayden, 2014; Keefe, 2006; Lucas, 2014). As we have already observed, few academic programmes deal with these issues in a systematic way.

From an effectiveness perspective, it could be argued that notions of "control" have to represent a cradle-to-grave approach across the HR function and that it requires an integrated approach towards dealing with the effective recruitment, selection, training, and exiting strategies for all employees. It could also be argued that the HR function is ill-prepared to deal with these task demands and that a significant programme of staff development would be needed to make certain that the HR function was itself effective in this regard. The threats from insiders is one that both highlights the vulnerabilities of the HR function within organisational effectiveness and the limitations of control systems. It also highlights its potential as a source of risk that could impair the performance of the organisation as a whole. Insider threats also raise another key issue around the toxic triangle, namely, how do we effectively identify and manage those colleagues who have damaging personality characteristics and who hold senior managerial positions? These are the employees who are often the most neglected part of this discourse.

Coming to a darkened workplace near you? Personality disorders and crisis

> […]. there are at least two ways that a personality characteristic can be called "dark" – in its nature or in its effects […]. We can claim that a personality concept is dark if it has a particularly malevolent character – individuals who have high elevations on the construct are motivated (consciously or unconsciously) to harm others (or themselves). On the other hand, a characteristic that has no particularly malevolent content could still have noxious consequences. […]. Harm, of some kind, is almost a necessary consequence of the label dark – (Spain *et al.*, 2014, p. S50).

The creation of harm in the workplace – whether by accident or intention – would normally be considered as a property of an inefficient organisation. Harm could be generated in various ways: by insiders with malicious intent; by outsiders who seek to cause harm; by the actions or inactions of managers who create an unsafe working environment; or by accidental causes which arise from failures in control systems. In virtually all of these cases, the interactions between people and processes are central to the conditions in which harm occurs. It could also be argued that the human resource function should play a role in seeking to prevent such harms from occurring, especially where they involve malevolent individuals, the training of staff around risk and security, and the development of a culture that facilitates the capture of information relating to early warnings and near misses. A consideration of a range of accidents and systems failures would suggest, however, that there are severe limitations to the abilities of the HR function to deal with these problems. This is especially the case when considering extreme cases of misbehaviour and the associated threats from insiders. The context in which these harms can be generated in the organisation can also be framed in terms of Padilla *et al.*'s (2007) "toxic triangle", where organisational leaders, especially those with negative and exploitative characteristics, can operate in an environment that allows them to manipulate and exploit those who work for them.

Organisations are only as secure as their human resources allow them to be. Weakness can exist as a function of the integrity and professionalism of those people within the organisation. It has been suggested, for example, that some 48 per cent of the data breaches within companies are caused by insiders (Verizon RISK Team and US Secret Service, 2010). The most recent examples of such breaches are provided by the data leaks carried out by Bradley Manning and Edward Snowden who both worked in

highly secure and trusted environments (Gurnow, 2014; Madar, 2013). In the Snowden case, this was an individual who had supposedly been vetted by his organisations and who was then able to by-pass multiple layers of controls in order to download and save a considerable amount of sensitive information to the press. Whilst Snowden is seen by some as a hero and whistle-blower (Harding, 2014), he has also been heavily criticised in government circles in both the UK and the USA (Hayden, 2014; Lucas, 2014; Terry, 2013). Of course, one might also question the initial government decisions taken around surveillance that seem to have prompted Snowden's actions in the first place. In particular, concerns could be expressed around the ethics of large-scale government surveillance programmes in a democratic society. One might also raise concerns around the motivations and abilities of the intelligence community to make sense of the information that they have collected, as well as the actions of governments in justifying the need for that data collection on such a scale (Brenner, 2013; Greewald, 2014; Tucker, 2014). These issues are, however, beyond the scope of this paper. It is also worth highlighting the fact that governments are not the only ones who engage in surveillance. Organisations who engage in the covert surveillance of its employees can also find their actions to be ethically problematic and there is a difficult balance to be struck between effective security and excessive intrusion. Again, this is an issue that is central to the interactions between people and processes around organisational effectiveness.

The underlying motivations for insiders are often expressed through the acronym MICE: money, ideology, coercion, and ego (Burkett, 2013). These drivers are often seen to lie at the core of explaining the various motivations of individuals to betray their organisations or even their countries. Of course Snowden was not the first case of a security professional leaking information to third parties. In the UK, the so-called Cambridge Five and the spy George Blake are well-known examples of security personnel who leaked sensitive and secret information to foreign powers (Hermiston, 2013; Kerr, 1996; Macintyre, 2014) and there was also a number of other alleged defections (Turchetti, 2003). Even the Manhattan Project to develop the atomic bomb was subject to information leaks (Herken, 1980; Picknett *et al.*, 2005). What differentiates the Snowden and Manning leaks is the scale of the information that was removed and the relative ease by which it could be stored on electronic media.

Changes in technology have also proved to be a critical factor in allowing information to be collected on "persons of interest" but they have also generated a new set of vulnerabilities for organisations around cyber attacks (Brenner, 2013). Cyber attacks have been carried out by corporate insiders, although much of this does not receive coverage by the mainstream media[3]. These insiders have invariably been recruited, selected, vetted, and trained by the organisation and, as stated earlier, the human resources function have a role to play in this process. The EU is the most "wired" part of the world, the source of a considerable amount of wealth, and with several jurisdictions for regulators to work over. As such, it is one of the most attractive geographical locations for cyber crime. For cyber criminals, the physical location of the asset to be stolen is not longer a constraint, as proximity is no longer needed to gain access to the information source. Location is important in terms of accessing the organisation's local network but in many cases even that might not require proximity. Where location does become important for cyber "criminals" is in terms of allowing unfettered access to the network whilst at the same time, avoiding the risks of detection and arrest by law enforcement. It is not a surprise, therefore, that cyber attacks are often launched from countries that provide adequate access to networks but do not

have strong levels of international collaboration around enforcement. Organised crime within Russia serves as an example of that activity (Holmes, 2008; Volkov, 2002), although there are considerable complexities and variations in the ways that organised crime operates in a global environment (Varese, 2011). In some cases, crime groups have also coerced organisational insiders through processes of social engineering as a means of gathering the "hostile" surveillance or details of the security protocols necessary to mount attacks (Colwill, 2009; Mitnick, 2011; Roy Sarkar, 2010).

This range of issues highlights the challenges that can arise out of the actions of individuals who have malevolent intent. These reflect the challenges that exist between the environmental threats facing the organisation, the role of internal leadership in mitigating (or generating) those threats, and the actions of other organisational members who act as followers or opponents of the dominant organisational culture. Figure 3 highlights some of the issues that emerge out of the interactions between some of the elements that relate to them. The issues highlighted are not meant to be inclusive of all of the characteristics that are associated with this toxic triangle but simply to highlight some of the problems that could very easily conspire to erode the development of organisational effectiveness. In this setting, management also has the potential to become the author of its own misfortune as many of the elements associated with a failure can be traced back to a range of dysfunctional behaviours that are generated by those leaders within the organisation who display "dark triad" (Jonason *et al.*, 2012; Paulhus and Williams, 2002) personality characteristics.

Research has highlighted the range of narcissistic, Machiavellian, and psychopathic behaviours that exist in organisations and the impact that they can have on organisational performance (Babiak and Hare, 2006; Campbell *et al.*, 2011; Jonason *et al.*, 2014; Padilla *et al.*, 2007; Smith and Lilienfeld, 2013). These so-called "dark triad" personality traits are typified by such characteristics (amongst other negative traits) as: a lack of empathy, a willingness to manipulate others (for self-betterment),

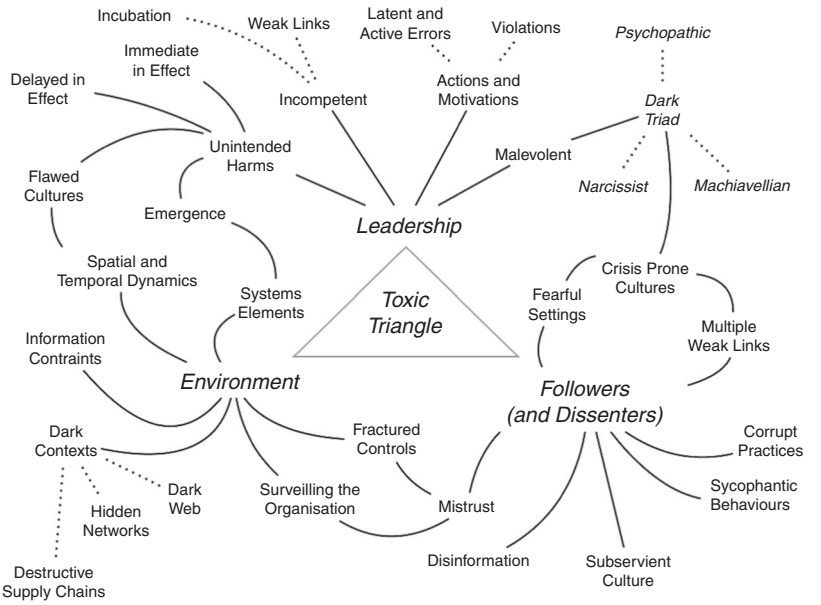


Figure 3.
Elements of the toxic triangle surrounding dysfunctional leadership

antagonism, and a belief in their own superiority (Conger, 1990; Paulhus and Williams, 2002; Spain *et al.*, 2014). In such cases they are considered to be especially harmful to the organisation given the positional power of the individuals concerned and are typified by:

> The systematic and repeated behaviour by a leader, supervisor or manager that violates the legitimate interest of the organisation by undermining and/or sabotaging the organisation's goals, tasks, resources, and effectiveness and/or the motivation, well-being or job satisfaction of subordinates – (Einarsen *et al.*, 2007, p. 208).

Clearly, these traits exist across the range of employees within the organisation. However, recent work has considered their prevalence amongst organisational leaders (Babiak and Hare, 2006). Concerns have also been expressed around the impact that these individuals can have in their search for power and self-promotion and how their own selfish agendas can impact on leadership strategies and organisational performance (Furnham *et al.*, 2012; Jonason *et al.*, 2012; Khoo and Burch, 2008).

The leadership styles of senior managers could have profound implications for effectiveness as they are held to translate into organisational structures and processes (Kets De Vries and Miller, 1984) and, in the case of weak managers, have also been seen to result in the appointments of staff who share the same characteristics (South and Matejka, 1990). One might also argue that narcissistic managers may look to appoint subordinates who will fuel their own needs, thereby creating a particular culture that would be self-reinforcing and therefore could ultimately be prone to crisis. A key implication here is that the temporal dynamics of these processes are important – some narcissists, for example, may prove to be constructive at certain points in time and within certain environmental settings as their self-serving behaviours may also support wider short-term organisational goals (Stein, 2013). There are also problems with those individuals who display sycophantic behaviours at lower levels of the organisation, but who then rise through the organisational hierarchy as a consequence (Pech and Slade, 2007). This is despite the fact that these individuals may sometimes be ill-suited to the tasks that they are required to undertake – what matters is their willingness to comply with the views of their leaders, irrespective of the validity of those views. The result is the creation of an organisational culture in which there is no effective challenge to the dominant mindset within the organisation. Ultimately this can create a toxic environment that runs through all levels of the organisational hierarchy where the decision makers suffer from the same form of paradigm blindness and where there is little, if any, scope for an alternative view, and which has the potential to incubate crisis. The result is often a form of resistance amongst the workforce which helps to generate the potential for crisis and failure.

The HR function within organisations should play a major role in identifying and acting upon such aberrant forms of behaviour. However, the history of organisational crises has illustrated that many of these organisational misbehaviours go unchecked. Research has investigated a range of these negative characteristics in such diverse areas as "celebrity", politics, banking (Boddy, 2011; Owen, 2008; Owen and Davidson, 2009; Pettman, 2010; Stein, 2000; Young and Pinsky, 2006), and even academia (Kornfeld, 2012; List *et al.*, 2001; Parker, 2014). This is especially the case were self-promotion and an increased media profile are seen as a means of achieving the positional power or outcomes that such individuals crave (Brunell *et al.*, 2011; Jensen *et al.*, 2002). Social media and electronic communications have also fuelled the opportunities that such narcissists have to promote their own self-importance

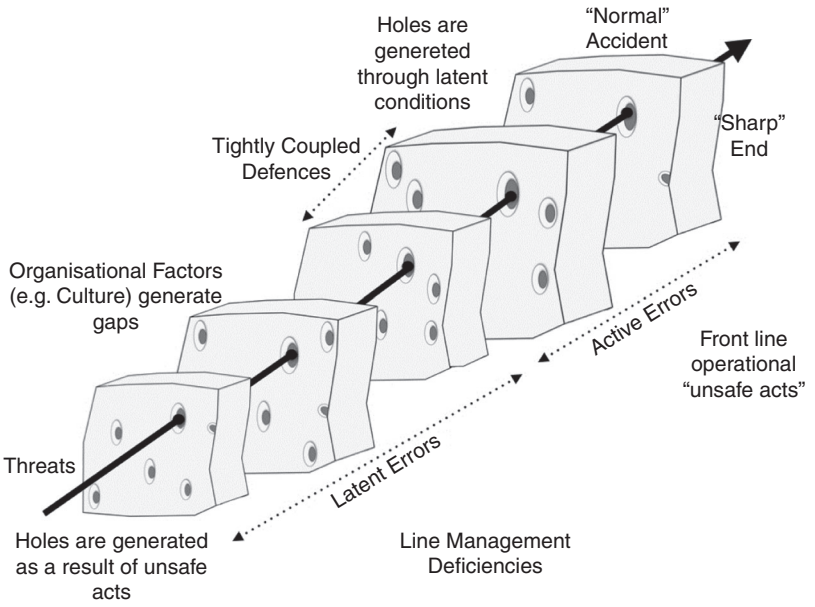
(Bergman *et al.*, 2011; Ong *et al.*, 2011). It has also provided the opportunities for individuals to engage in new forms of misbehaviours around cyber harassment and cyber loafing (Henle *et al.*, 2009; Whitty and Carr, 2006; Wishart, 2014).

The combination of social media and dark personality characteristics is a potentially toxic combination and one that clearly has the potential to harm an organisation's reputation. Social media has also been a factor in shaping a set of deviant behaviours around child abuse (most notably through grooming), radicalisation, and a range of other unacceptable behaviours (Kierkegaard, 2008; Whittle *et al.*, 2013) and these have created an additional set of concerns for those organisations and agencies who seek to prevent such abuse occurring (Conway and McInerney, 2008; Torok, 2013; Whittle *et al.*, 2013).

The recruitment of people with dark triad personalities has also highlighted the need to attempt an identification of these characteristics early in the process; and this is more pronounced in some key professions where the potential for harm is high (perhaps most notably medicine) (Knights and Kennedy, 2007; van Mook *et al.*, 2010). Within the UK, the manner in which so-called "problem doctors" (Donaldson, 1994; Rosenthal, 1997) has become an issue within healthcare resulted in a major government initiative around the management of adverse events (DoH, 2000, 2001, 2003). Much of this concern was around finding systems-based approaches to determining the effective management of patient treatment and the reduction of human errors and violations (Reason, 2001; Redfern *et al.*, 2000; Rosenthal, 1987, 1995). A particular case that had widespread effects was that of Dr Harold Shipman who murdered in the order of 215[4] of his patients before being apprehended by police. Shipman was able to exploit multiple failures in the control systems that were in place around prescribing drugs, the signing of death certificates, and the difficulties of monitoring and controlling single-handed GP practices (Sitford, 2000; Smith, 2002a, b).

The ability to identify and by-pass organisational defences is a key factor in the strategies of the malevolent individual to cause harm in organisations. This applies to third parties who seek to attack the organisation from outside as well as to those insiders who cause harm by either accidental or intentional effects. Figure 4 sets out Reason's so-called "Swiss Cheese" model, in which he uses the analogy to highlight the gaps that exist within organisational defences. These gaps can either be generated by the latent conditions of managers – by failing to maintain and test defences, or by the generation of an organisational culture that allows for lax practices – or by the direct actions of individuals. In the case of Shipman, it was a combination of these factors that allowed him to overcome the various procedures that were in place to protect patients. It was the trust given to doctors that was instrumental in allowing him to kill without detection over such a long period of time. That notion of trust was manifest in both the perceptions of both patients and colleagues who would struggle to conceive of a doctor as being capable of murder, and this worked in combination with the procedures that were in place to control the prescription and retention of potentially dangerous drugs to allow him to stockpile diamorphine and use it to kill his patients. Given that Shipman had been found guilty of obtaining prescription drugs for his own use early in his career (Smith, 2002a), then such a level of trust would, in hindsight, seem to be somewhat misplaced.

Healthcare is not the only organisational sector that has experienced problems in terms of the threats from insiders. There have been several examples where individuals have been involved in workplace violence, sabotage, data theft, the identification of organisational vulnerabilities, as well as a range of attempts to defraud organisations



Source: Adapted from information in Reason (1990a, b, 1995, 1997)

Figure 4.
Reason's Swiss Cheese model

(Ambrose *et al.*, 2002; Bentley *et al.*, 2014; Dhillon and Moores, 2001; Greener, 2006). The problems concerning the presentation of company accounts at Tesco in September 2014 was also a result of the actions of insiders – in this case, it was alleged that they were senior managers who conspired to make the accounts appear more favourable (Butler and Treanor, 2014; Pratley, 2014; Wood and Farrell, 2014). The implications associated with this range of organisational misbehaviours are considerable and it illustrates the processes by which effectiveness can be impaired. First, it can be damaged by the direct, intentional, and malevolent actions of individuals who ultimately seek to cause harm; and second, by the accidental effects caused by the actions of individuals where the emergent consequences of those behaviours cause harm by reputational damage (Spain *et al.*, 2014). In one case, the generation of harms is intentional, and in the other it is an emergent effect arising out of misbehaviours and unprofessional behaviours where harm is a secondary consequence. The challenge for HRM is to manage the range of potential problems arising from such misbehaviours within the workplace and to develop the dynamic capabilities within the HR function that would allow it to deal with the task demands generated by such misbehaviours.

Conclusions

> The pattern which connects […]. is a metapattern, a pattern of patterns. More often than not we fail to see it […]. we have been trained to think of patterns as fixed affairs. The truth is that the right way to begin to think about the pattern which connects is as a dance of interacting parts, secondarily pegged down by various sorts of physical limits and by habits, and by the naming of states and component entities – (Bateson, cited in Goleman, 1985, p. 7).

The management of uncertainty is an important element of the determination of effectiveness. The manner in which organisations can incorporate the various forms of

knowledge into their strategy is a key element in this process. The categorisation of knowledge used by former US Secretary of Defence Donald Rumsfeld is a useful starting point in this context. Rumsfeld argued that there are the core things that we know and understand (the knowns), the things that we know that we do not know and understand (the known unknowns), and those issues that we haven't even considered as problematic (the unknown unknowns) (Rumsfeld, 2002, 2011). The development of organisational effectiveness ultimately requires managers to recognise the limitations of their own knowledge when making decisions – that is, to reflect on the parameters and significance of the known unknowns whilst acknowledging that even the knowns are often spatially and temporally bounded. In some cases, what we think of as a "known" phenomena (and, therefore, by implication understood) or a course of action may well not work in a different context. Even within those elements that we understand, the potential for emergence is a key factor in the behaviour (and performance) of socio-technical systems. This is particularly the case around the interactions between innovation and risk. As organisations innovate they change the parameters of the system and therefore generate the potential for emergent conditions. In Rumsfeld's terms, these incorporate more of the unknowns (both known and unknown) and have the potential to create new conditions for the organisation to respond to. This movement into areas where the knowledge base is less robust is an essential component of the development of organisations over time but it also generates some challenges around the ways in which it generates additional risks.

The "dance of interacting parts" as outlined by Bateson is an apt way of describing many of the process elements that take place around the creation and erosion of effectiveness. The failure to manage the uncertainty that is inherent in the decision-making process is a key element of the generation of organisational failures and one that is exacerbated by the interactions between people and processes. Where the performance of people is rendered problematic as a function of their dark triad personality characteristics, and where the processes around control are flawed, then this uncertainty is increased.

As noted earlier, and as a response to Sparrow and Cooper's (2014) call for a more multi-disciplinary approach towards dealing with the range of challenges facing organisational effectiveness, this paper has sought to outline elements of the darker side of organisational effectiveness by focusing on a range of issues that have the potential to move the organisation into a state of crisis and which also have the issues of people and performance at their core. However, there is a need to add a note of caution to any calls towards a multi-disciplinary approach. The Academy needs to ensure that it does not engage in a process of academic grazing – where researchers move beyond their domain of knowledge and simply capture ideas and concepts from other disciplines without grounding those concepts in the debates and challenges of their host discipline. Many of the real-world problems facing organisations require research that transcends academic silos and seeks to analyse the problem through different analytical lenses. Herein lies the paradox for our own "effectiveness" as a community of researchers. How do we deal with the demands for a multi-disciplinary approach whilst ensuring that we have sufficient fluency in other disciplines to be effective in working with those concepts.

This is particularly problematic in the performance-based environment of the Research Excellence Framework in the UK (and similar programmes elsewhere) where the demands to publish papers in highly ranked journals can have the effect of stifling innovation and theoretical development around multi-level issues. Multi-disciplinary research is slow and often laborious. It requires a commitment to life-long learning that is often preached by universities but often not fully encouraged within their own staff.

If we are to make a contribution to the problems facing organisations, then the Academy itself must change in order to produce the next generation of scholars who are capable of working in such an environment. This Journal has a major contribution to make in the development of concepts and challenges that will shape those debates, but only if we see effectiveness as a double-edge issue where the potential for failure is closely related to the search for high levels of performance. By concentrating on the latter we might be unwittingly be generating the former.

Acknowledgements

The author would like to acknowledge the comments made on an earlier version of this paper by Robert McMaster and Moira Fischbacher-Smith. Needless to say, all errors of omission and commission remain those of the author apart from those generated by latent conditions over which the author had no control. The work underpinning this paper was supported by a grant from the EPSRC (Grant EP/G004307/1) relating to organisational vulnerabilities.

Notes

1. The content of 20 masters programmes in HRM was examined at random to see if there was any explicit coverage of issues of risk (including health and safety) or crisis. Only Strathclyde University had a full optional module in risk management that was evident from the course descriptors for its HRM programme.
2. See the course web page at: www.strath.ac.uk/hrm/courses/postgraduate/pg-fulltime/structure/
3. These were points made by members of the US and EU security and police agencies who made the comments under Chatham House rules. As a consequence they cannot have the comments attributed to them.
4. It is doubtful that the true scale of Shipman's crimes will ever be accurately known due to the time period involved. It is possible that he killed in excess of 215 patients.

References

Ackroyd, S. and Thompson, P. (1999), *Organizational Misbehaviour*, SAGE, London.

Ambrose, M.L., Seabright, M.A. and Schminke, M. (2002), "Sabotage in the workplace: the role of organizational injustice", *Organizational Behavior and Human Decision Processes*, Vol. 89 No. 1, pp. 947-965.

Ashby, W.R. (1958), "Requisite variety and its implications for the control of complex systems", *Cybernetica*, Vol. 1 No. 2, pp. 83-99.

Ashby, W.R. (1962), "Principles of the self-organizing system", in Von Foerster, H. and Zopf, G.W. (Eds), *Principles of Self-Organization: Transactions of the University of Illinois Symposium*, Pergamon Press, London, pp. 255-278.

Babiak, P. and Hare, R.D. (2006), *Snakes in Suits: When Psychopaths go to Work*, Harper Collins Publishers, New York, NY.

Bentley, T.A., Catley, B., Forsyth, D. and Tappin, D. (2014), "Understanding workplace violence: the value of a systems perspective", *Applied Ergonomics*, Vol. 45 No. 4, pp. 839-848.

Bergen, P. and Reynolds, A. (2005), "Blowback revisited. Today's insurgents are tomorrow's terrorists", *Foreign Affairs*, Vol. 84 No. 6, pp. 2-6.

Bergman, S.M., Fearrington, M.E., Davenport, S.W. and Bergman, J.Z. (2011), "Millennials, narcissism, and social networking: what narcissists do on social networking sites and why", *Personality and Individual Differences*, Vol. 50 No. 5, pp. 706-711.

Berry, A.J., Coad, A.F., Harris, E.P., Otley, D.T. and Stringer, C. (2009), "Emerging themes in management control: a review of recent literature", *The British Accounting Review*, Vol. 41 No. 1, pp. 2-20.

Boddy, C. (2011), "The corporate psychopaths theory of the global financial crisis", *Journal of Business Ethics*, Vol. 102 No. 2, pp. 255-259.

Brenner, J. (2013), *Glass Houses. Privacy, Secrecy, and Cyber Insecurity in a Transparent World*, Pengiun Books, New York, NY.

Brown, A.D. (2005), "Making sense of the collapse of barings bank", *Human Relations*, Vol. 58 No. 12, pp. 1579-1604.

Brunell, A.B., Staats, S., Barden, J. and Hupp, J.M. (2011), "Narcissism and academic dishonesty: the exhibitionism dimension and the lack of guilt", *Personality and Individual Differences*, Vol. 50 No. 3, pp. 323-328.

Burkett, R. (2013), "An alternative framework for agent recruitment: from MICE to RASCLS", *Studies in Intelligence*, Vol. 57 No. 1, pp. 7-17.

Burnett, J.J. (1998), "A strategic approach to managing crises", *Public Relations Review*, Vol. 24 No. 4, pp. 475-488.

Butler, S. and Treanor, J. (2014), "Pressure mounts on Tesco chairman as the second biggest shareholder reduces stake", *The Guardian*, 25 September, p. 29.

Campbell, W.K., Hoffman, B.J., Campbell, S.M. and Marchisio, G. (2011), "Narcissism in organizational contexts", *Human Resource Management Review*, Vol. 21 No. 4, pp. 268-284.

Carmeli, A. and Schaubroeck, J. (2006), "Top management team behavioral integration, decision quality, and organizational decline", *The Leadership Quarterly*, Vol. 17 No. 5, pp. 441-453.

Collingridge, D. (1984), "Lessons of nuclear power US and UK history", *Energy Policy*, Vol. 12 No. 1, pp. 46-67.

Colwill, C. (2009), "Human factors in information security: the insider threat – who can you trust these days?", *Information Security Technical Report*, Vol. 14 No. 4, pp. 186-196.

Conger, J.A. (1990), "The dark side of leadership", *Organizational Dynamics*, Vol. 19 No. 2, pp. 44-55.

Conway, M. and McInerney, L. (2008), "Jihadi video and auto-radicalisation: evidence from an exploratory youtube study", in Ortiz-Arroyo, D., Larsen, H., Zeng, D., Hicks, D. and Wagner, G. (Eds), *Intelligence and Security Informatics*, Vol. 5376, Springer, Berlin and Heidelberg, pp. 108-118.

Day, M. (2007), "Doctors held for bombing attempts, but NHS defends vetting procedures", *BMJ*, Vol. 335 No. 7609, p. 9.

Dhillon, G. and Moores, S. (2001), "Computer crimes: theorizing about the enemy within", *Computers & Security*, Vol. 20 No. 8, pp. 715-723.

Ditillo, A. (2004), "Dealing with uncertainty in knowledge-intensive firms: the role of management control systems as knowledge integration mechanisms", *Accounting, Organizations and Society*, Vol. 29 Nos 3/4, pp. 401-421.

DoH (2000), *An Organisation with a Memory: Report of an Expert Group on Learning From Adverse Events in the NHS Chaired by the Chief Medical Officer*, The Stationary Office, London.

DoH (2001), *Building a Safer NHS for Patients. Implementing an Organisation with a Memory*, Department of Health, London.

DoH (2003), *Design for Patient Safety: A System-Wide Design-Led Approach to Tackling Patient Safety in the NHS*, Department of Health/The Design Council, London.

Donaldson, L. (1994), "Doctors with problems in an NHS workforce", *British Medical Journal*, Vol. 308 No. 6939, pp. 1277-1282.

Eichener, V. (1997), "Effective European problem-solving: lessons from the regulation of occupational safety and environmental protection", *Journal of European Public Policy*, Vol. 4 No. 4, pp. 591-608.

Einarsen, S., Aasland, M.S. and Skogstad, A. (2007), "Destructive leadership behaviour: a definition and conceptual model", *The Leadership Quarterly*, Vol. 18 No. 3, pp. 207-216.

Eisenhardt, K.M. and Martin, J.M. (2000), "Dynamic capabilities: what are they?", *Strategic Management Journal*, Vol. 21 Nos 10/11, pp. 1105-1121.

Engelen, E. (2001), "Globalisation and multilevel governance in Europe: realist criteria for institutional design, or how pessimistic should one be?", *Critical Review of International Social and Political Philosophy*, Vol. 4 No. 1, pp. 131-156.

Eriksson, K. and McConnell, A. (2011), "Contingency planning for crisis management: recipe for success or political fantasy?", *Policy and Society*, Vol. 30 No. 2, pp. 89-99.

Furnham, A., Trickey, G. and Hyde, G. (2012), "Bright aspects to dark side traits: dark side traits associated with work success", *Personality and Individual Differences*, Vol. 52 No. 8, pp. 908-913.

Goleman, D. (1985), *Vital Lies, Simple Truths. The Psychology of Self-Deception*, Simon & Schuster Paperbacks, New York, NY.

Greener, I. (2006), "Nick leeson and the collapse of barings bank: socio-technical networks and the 'rogue trader' ", *Organization*, Vol. 13 No. 3, pp. 421-441.

Greewald, G. (2014), *No Place to Hide. Edward Snowden, the NSA and the Surveillance State*, Hamish Hamilton (Pengiun Group), London.

Gurnow, M. (2014), *The Edward Snowden Affair. Exposing the Politics and Media Behind the NSA Scandal*, Indianapolis, Blue River Press.

Harding, L. (2014), *The Snowden Files. The Inside Story of the World's Most Wanted Man*, Guardian Books, London.

Hayden, M.V. (2014), "Beyond snowden", *World Affairs*, Vol. 176 No. 5, pp. 13-23.

Henle, C.A., Kohut, G. and Booth, R. (2009), "Designing electronic use policies to enhance employee perceptions of fairness and to reduce cyberloafing: an empirical test of justice theory", *Computers in Human Behavior*, Vol. 25 No. 4, pp. 902-910.

Herken, G. (1980), " 'A Most deadly illusion': the atomic secret and American nuclear weapons policy, 1945-1950", *Pacific Historical Review*, Vol. 49 No. 1, pp. 51-76.

Hermiston, R. (2013), *The Greatest Traitor. The Secret Lives of Agent George Blake*, Aurum Press, London.

Hodge, B. and Coronado, G. (2007), "Understanding change in organizations in a far-from-equilibrium world", *Emergence: Complexity and Organizations*, Vol. 9 No. 3, pp. 3-15.

Holmes, L. (2008), "Corruption and organised crime in Putin's Russia", *Europe-Asia Studies*, Vol. 60 No. 6, pp. 1011-1031.

Jensen, L.A., Arnett, J.J., Feldman, S.S. and Cauffman, E. (2002), "It's wrong, but everybody does it: academic dishonesty among high school and college students", *Contemporary Educational Psychology*, Vol. 27 No. 2, pp. 209-228.

Jonason, P.K., Slomski, S. and Partyka, J. (2012), "The dark triad at work: how toxic employees get their way", *Personality and Individual Differences*, Vol. 52 No. 3, pp. 449-453.

Jonason, P.K., Wee, S., Li, N.P. and Jackson, C. (2014), "Occupational niches and the dark triad traits", *Personality and Individual Differences*, Vol. 69, October, pp. 119-123.

Keefe, P.R. (2006), *Chatter. Uncovering the Echelon Surveillence Network and the Secret World of Global Eavesdropping*, Random House, New York, NY.

Kerr, S. (1996), "KGB sources on the Cambridge network of Soviet agents: true or false?", *Intelligence and National Security*, Vol. 11 No. 3, pp. 561-585.

Kets De Vries, M.F.R. and Miller, D. (1984), "Neurotic style and organizational pathology", *Strategic Management Journal*, Vol. 5 No. 1, pp. 35-55.

Khoo, H.S. and Burch, G.S.J. (2008), "The 'dark side' of leadership personality and transformational leadership: an exploratory study", *Personality and Individual Differences*, Vol. 44 No. 1, pp. 86-97.

Kierkegaard, S. (2008), "Cybering, online grooming and ageplay", *Computer Law & Security Review*, Vol. 24 No. 1, pp. 41-55.

Knights, J.A. and Kennedy, B.J. (2007), "Medical school selection: impact of dysfunctional tendencies on academic performance", *Medical Education*, Vol. 41 No. 4, pp. 362-368.

Kornfeld, D.S. (2012), "Perspective: research misconduct: the search for a remedy", *Academic Medicine*, Vol. 87 No. 7, pp. 877-882.

Kraemer, S. and Carayon, P. (2007), "Human errors and violations in computer and information security: the viewpoint of network administrators and security specialists", *Applied Ergonomics*, Vol. 38 No. 2, pp. 143-154.

Kramer, L.A. and Heuer, R.J. (2007), "America's increased vulnerability to insider espionage", *International Journal of Intelligence and Counter Intelligence*, Vol. 20 No. 1, pp. 50-64.

LaPorte, T.R. and Consolini, P.M. (1991), "Working in practice but not in theory: theoretical challenges of 'high-reliability organizations'", *Journal of Public Administration Research and Theory: J-PART*, Vol. 1 No. 1, pp. 19-48.

List, J.A., Bailey, C.D., Euzent, P.J. and Martin, T.L. (2001), "Academic economists behaving badly? A survey on three areas of unethical behavior", *Economic Inquiry*, Vol. 39 No. 1, pp. 162-170.

Lucas, G.R.J. (2014), "NSA management directive #424: secrecy and privacy in the aftermath of edward snowden", *Ethics & International Affairs*, Vol. 28 No. 1, pp. 29-38.

Macintyre, B. (2014), *A Spy Amongst Friends. Kim Philby and the Great Betrayal*, Bloomsbury, London.

Madar, C. (2013), *The Passion of Bradley Manning. The Story Behind the Wikileaks Whistleblower*, Verso, London.

Mitnick, K. (2011), *Social Engineering. The Art of Human Hacking*, Wiley Publishing Inc, Indianapolis, IN.

Mitroff, I.I., Pauchant, T.C., Finney, M. and Pearson, C. (1989), "Do (some) organizations cause their own crises? Culture profiles of crisis prone versus crisis prepared organizations", *Industrial Crisis Quarterly*, Vol. 3, pp. 269-283.

Ong, E.Y.L., Ang, R.P., Ho, J.C.M., Lim, J.C.Y., Goh, D.H., Lee, C.S. and Chua, A.Y.K. (2011), "Narcissism, extraversion and adolescents' self-presentation on facebook", *Personality and Individual Differences*, Vol. 50 No. 2, pp. 180-185.

Owen, D. (2008), *In Sickness and in Power*, Methuen, London.

Owen, D. and Davidson, J. (2009), "Hubris syndrome: an acquired personality disorder? A study of US Presidents and UK Prime Ministers over the last 100 years", *Brain*, Vol. 132 No. 5, pp. 1396-1406.

Padilla, A., Hogan, R. and Kaiser, R.B. (2007), "The toxic triangle: destructive leaders, susceptible followers, and conducive environments", *The Leadership Quarterly*, Vol. 18 No. 3, pp. 176-194.

Parker, M. (2014), "University, Ltd: changing a business school", *Organization*, Vol. 21 No. 2, pp. 281-292.

Pauchant, T.C. and Mitroff, I.I. (1990), "Crisis management: managing paradox in a chaotic world", *Technological Forecasting and Social Change*, Vol. 38 No. 2, pp. 117-134.

Pauchant, T.C. and Mitroff, I.I. (1992), *Transforming the Crisis-Prone Organization. Preventing Individual Organizational and Environmental Tragedies*, Jossey-Bass Publishers, San Fransisco, CA.

Paulhus, D.L. and Williams, K.M. (2002), "The dark triad of personality: narcissism, machiavellianism, and psychopathy", *Journal of Research in Personality*, Vol. 36 No. 6, pp. 556-563.

Pech, R.J. and Slade, B.W. (2007), "Organisational sociopaths: rarely challenged, often promoted", *Why? Society and Business Review*, Vol. 2 No. 3, pp. 254-269.

Pena, C.V. (2002), "Blowback: the unintended consequences of military tribunals", *Notre Dame Journal of Law, Ethics & Public Policy*, Vol. 16 No. 1, pp. 119-132.

Perrow, C. (2009), "What's needed is application, not reconciliation: a response to Shrivastava, Sonpar and Pazzaglia (2009)", *Human Relations*, Vol. 62 No. 9, pp. 1391-1393.

Pettman, R. (2010), "Psychopathology and world politics", *Cambridge Review of International Affairs*, Vol. 23 No. 3, pp. 475-492.

Piattoni, S. (2009), "Multi-level governance: a historical and conceptual analysis", *Journal of European Integration*, Vol. 31 No. 2, pp. 163-180.

Picknett, L., Prince, C., Prior, S. and Brydon, R. (2005), *Friendly Fire. The Secret war Between the Allies*, Mainstream Publishing, Edinburgh.

Power, R. and Forte, D. (2006), "Thwart the insider threat: a proactive approach to personnel security", *Computer Fraud & Security*, Vol. 2006 No. 7, pp. 10-15.

Pratley, N. (2014), "Analysis. It is either a shambles or a scandal. Both reflect badly on the leadership", *The Guardian*, 25 September, p. 29.

Quinn, R.E. and Cameron, K. (1983), "Organizational life cycles and shifting criteria of effectiveness: some preliminary evidence", *Management Science*, Vol. 29 No. 1, pp. 33-51.

Quinn, R.E. and Rohrbaugh, J. (1983), "A spatial model of effectiveness criteria: towards a competing values approach to organizational analysis", *Management Science*, Vol. 29 No. 3, pp. 363-377.

Reason, J.T. (1990a), "The contribution of latent human failures to the breakdown of complex systems", *Philosophical Transactions of the Royal Society of London, B*, Vol. 327 No. 1241, pp. 475-484.

Reason, J.T. (1990b), *Human Error*, Oxford University Press, Oxford.

Reason, J.T. (1995), "Understanding adverse events: human factors", *Quality in Health Care*, Vol. 4 No. 2, pp. 80-89.

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

Reason, J.T. (2001), "Understanding adverse events: the human factor", in Vincent, C. (Ed.), *Clinical Risk Management. Enhancing Patient Safety*, 2nd ed., BMJ Books, London, pp. 9-30.

Reason, J.T. (2008), *The Human Condition. Unsafe Acts, Accidents and Heroic Recoveries*, Ashgate, Farnham.

Redfern, M., Keeling, J. and Powell, E. (2000), *The Royal Liverpool Children's Inquiry Report*, The Stationary Office, London.

Roberts, K.H., Bea, R. and Bartles, D.L. (2001), "Must accidents happen? Lessons from high-reliability organizations", *The Academy of Management Executive*, Vol. 15 No. 3, pp. 70-78.

Roberts, K.H., Rousseau, D.M. and La Porte, T.R. (1994), "The culture of high reliability: quantitative and qualitative assessment aboard nuclear-powered aircraft carriers", *The Journal of High Technology Management Research*, Vol. 5 No. 1, pp. 141-161.

Rosenthal, M.M. (1987), *Dealing with Medical Malpractice: The British and Swedish Experience*, Tavistock, London.

Rosenthal, M.M. (1995), *The Incompetent Doctor*, Open University Press, Milton Keynes.

Rosenthal, M.M. (1997), "Promise and reality: professional self-regulation and 'problem' colleagues", in Lens, P. and van der Wal, G. (Eds), *Problem Doctors. A Conspiracy of Silence*, IOS Press, Amsterdam, pp. 9-29.

Rousseau, D.M. (1985), "Issues of level in organizational research: multi-level and cross-level perspectives", *Research in Organizational Behavior*, Vol. 7 No. 1, pp. 1-37.

Roy Sarkar, K. (2010), "Assessing insider threats to information security using technical, behavioural and organisational measures", *Information Security Technical Report*, Vol. 15 No. 3, pp. 112-133.

Rumsfeld, D. (2002), "DoD news briefing – Secretary Rumsfeld and Gen. Myers", News Transcript, Office of the Assistant Secretary of Defense (Public Affairs), US Department of Defense, Washington, DC, available at: www.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636 (accessed 17 August 2011).

Rumsfeld, D. (2011), *Known and Unknown. A Memoir*, Sentinel, New York, NY.

Sagan, S.D. (1993), *The Limits of Safety. Organizations, Accidents, and Nuclear Weapons*, Princeton University Press, Princeton, NJ.

Scharpf, F.W. (1997), "Introduction: the problem-solving capacity of multi-level governance", *Journal of European Public Policy*, Vol. 4 No. 4, pp. 520-538.

Sheaffer, Z. and Mano-Negrin, R. (2003), "Executives' Orientations as indicators of crisis management policies and practices", *Journal of Management Studies*, Vol. 40 No. 2, pp. 573-606.

Shrivastava, S., Sonpar, K. and Pazzaglia, F. (2009), "Normal accident theory versus high reliability theory: a resolution and call for an open systems view of accidents", *Human Relations*, Vol. 62 No. 9, pp. 1357-1390.

Simpson, C. (1988), *Blowback: America's Recruitment of Nazis and its Effects on the Cold War*, Weidenfeld & Nicolson, New York, NY.

Sitford, M. (2000), *Addicted to Murder – the True Story of Dr Harold Shipman*, Virgin Publishing, London.

Smith, D. (2000), "Crisis management teams: issues in the management of operational crises", *Risk Management: An International Journal*, Vol. 2 No. 3, pp. 61-78.

Smith, D. (2002a), "Not by error, but by design – Harold Shipman and the regulatory crisis for health care", *Public Policy and Administration*, Vol. 17 No. 4, pp. 55-74.

Smith, D. (2004), "For whom the bell tolls: imagining accidents and the development of crisis simulation in organisations", *Simulation and Gaming*, Vol. 35 No. 3, pp. 347-362.

Smith, D. and Elliott, D. (2007), "Exploring the barriers to learning from crisis: organizational learning and crisis", *Management Learning*, Vol. 38 No. 5, pp. 519-538.

Smith, J. (2002b), *The Shipman Inquiry. First Report*, The Shipman Inquiry, Manchester.

Smith, S.F. and Lilienfeld, S.O. (2013), "Psychopathy in the workplace: the knowns and unknowns", *Aggression and Violent Behavior*, Vol. 18 No. 2, pp. 204-218.

Snell, S.A. and Youndt, M.A. (1995), "Human resource management and firm performance: testing a contingency model of executive controls", *Journal of Management*, Vol. 21 No. 4, pp. 711-737.

South, J.C. and Matejka, K. (1990), "Unmasking multiple weak links in the chain of command", *Management Decision*, Vol. 28 No. 3, pp. 22-26.

Spain, S.M., Harms, P. and LeBreton, J.M. (2014), "The dark side of personality at work", *Journal of Organizational Behavior*, Vol. 35 No. S1, pp. S41-S60.

Sparrow, P. and Cooper, C. (2014). Organizational effectiveness, people and performance: new challenges, new research agendas", *Joural of Organizational Effectiveness: People and Performance*, Vol. 1 No. 1, pp. 2-13.

Stein, M. (2000), "The risk taker as shadow: a psychoanlytic view of the collapse of barings bank", *Journal of Management Studies*, Vol. 37 No. 8, pp. 1215-1230.

Stein, M. (2013), "When does narcissistic leadership become problematic? Dick Fuld at Lehman Brothers", *Journal of Management Inquiry*, Vol. 22 No. 3, pp. 282-293.

Streatfield, P.J. (2001). *The Paradox of Control in Organizations*, Routledge, London.

Sutcliffe, K.M. (2011), "High reliability organizations (HROs)", *Best Practice & Research Clinical Anaesthesiology*, Vol. 25 No. 2, pp. 133-144.

Teece, D.J. (2014), "A dynamic capabilities-based entrepreneurial theory of the multinational enterprise", *J Int Bus Stud*, Vol. 45 No. 1, pp. 8-37.

Teece, D.J., Pisano, G. and Shuen, A. (1997), "Dynamic capabilities and strategic management", *Strategic Management Journal*, Vol. 18 No. 7, pp. 509-533.

Tenner, E. (1996), *Why Things Bite Back. Technology and the Revenge Effect*, Fourth Estate, London.

Terry, S.M. (2013), "How to prevent the next Edward Snowden", *Foreign Affairs*, 17 June, available at: www.foreignaffairs.com/articles/139516/sue-mi-terry/how-to-prevent-the-next-edward-snowden (accessed 19 June 2014).

Thompson, P. (2011), "The trouble with HRM", *Human Resource Management Journal*, Vol. 21 No. 4, pp. 355-367.

Thompson, P. and van den Broek, D. (2010), "Managerial control and workplace regimes: an introduction", *Work, Employment & Society*, Vol. 24 No. 3, pp. 1-12.

Torok, R. (2013), "Developing an explanatory model for the process of online radicalisation and terrorism", *Security Informatics*, Vol. 2 No. 1, pp. 1-10.

Tsoukas, H. (1997), "The tyranny of light: the temptations and the paradoxes of the information society", *Futures*, Vol. 29 No. 9, pp. 827-843.

Tsoukas, H. (1999), "David and Goliath in the risk society: making sense of the conflict between shell and greenpeace in the North Sea", *Organization*, Vol. 6 No. 3, pp. 499-528.

Tsoukas, H. and Chia, R. (2002), "On organizational becoming: rethinking organizational change", *Organization Science*, Vol. 13 No. 5, pp. 567-582.

Tucker, D. (2014), *The End of Intelligence. Espionage and State Power in the Information Age*, Stanford University Press, Stanford, CA.

Turchetti, S. (2003), "Atomic secrets and governmental lies: nuclear science, politics and security in the pontecorvo case", *The British Journal for the History of Science*, Vol. 36 No. 04, pp. 389-415.

Turner, B.A. (1976), "The organizational and interorganizational development of disasters", *Administrative Science Quarterly*, Vol. 21 No. 3, 378-397.

Turner, B.A. (1978), *Man-Made Disasters*, Wykeham, London.

Turner, B.A. (1994), "The causes of disaster: sloppy management", *British Journal of Management*, Vol. 5 No. 3, pp. 215-219.

Turner, K.L. and Makhija, M.V. (2006), "The role of organizational controls in managing knowledge", *Academy of Management Review*, Vol. 31 No. 1, pp. 197-217.

van Mook, W.N.K.A., Gorter, S.L., De Grave, W.S., van Luijk, S.J., Wass, V., Zwaveling, J.H., Schuwirth, L.W. and Van Der Vleuten, C.P.M. (2010), "Bad apples spoil the barrel: addressing unprofessional behaviour", *Medical Teacher*, Vol. 32 No. 11, pp. 891-898.

Varese, F. (2011), *Mafias on the Move. How Organized Crime Conquers new Territories*, Princeton University Press, Princeton, NJ.

Verizon RISK Team and US Secret Service (2010), *2010 Data Breach Investigations Report*, Verizon Risk Team.

Vogel, D. (1997), "Trading up and governing across: transnational governance and environmental protection", *Journal of European Public Policy*, Vol. 4 No. 4, pp. 556-571.

Volkov, V. (2002), *Violent Entrepreneurs. The use of Force in the Making of Russian Capitalism*, Cornell University Press, Ithica, NY.

Whittle, H., Hamilton-Giachritsis, C., Beech, A. and Collings, G. (2013), "A review of online grooming: characteristics and concerns", *Aggression and Violent Behavior*, Vol. 18 No. 1, pp. 62-70.

Whitty, M.T. and Carr, A.N. (2006), "New rules in the workplace: applying object-relations theory to explain problem internet and email behaviour in the workplace", *Computers in Human Behavior*, Vol. 22 No. 2, pp. 235-250.

Winter, S.G. (2003), "Understanding dynamic capabilities", *Strategic Management Journal*, Vol. 24 No. 10, pp. 991-995.

Wishart, R. (2014), "'Cybernat' attacks on JK Rowling won't sway Scottish voters", *The Guardian*, 12 June, available at: www.theguardian.com/commentisfree/2014/jun/2012/cybernat-attack-jk-rowling-scottish-voters-online-abuse-scottish-independence (accessed 17 September 2014).

Wood, Z. and Farrell, S. (2014), "£2bn shares slide as Tesco admits overstating profits", *The Guardian*, 23 September, pp. 1-4.

Woodford, M. (2012), *Exposure. Inside the Olympus Scandal*, Portfolio Penguin, London.

Young, M.S. and Pinsky, D. (2006), "Narcissism and celebrity", *Journal of Research in Personality*, Vol. 40 No. 5, pp. 463-471.

Corresponding author
Professor Denis Fischbacher-Smith can be contacted at: denis.fischbacher-smith@glasgow.ac.uk