AN EVALUATION OF THE READINESS OF UK COMPANIES FOR DISRUPTIONS IN ENERGY SUPPLY (1996 – 2006)

By
James R. Young

A dissertation submitted to

in partial fulfillment of the requirements for a degree of :

Master of Business Administration

2007

Email:james@envisionltd.com

A Dissertation entitled

AN EVALUATION OF THE READINESS OF UK COMPANIES FOR DISRUPTIONS IN ENERGY SUPPLY

By

James R Young

We hereby certify that this Dissertation submitted by James R Young conforms to acceptable standards and as such is fully adequate in scope and quality. It is therefore approved as the fulfillment of the Dissertation requirements for the degree of Master of Business Administration.

Approved:

Dissertation Advisor (Dr Bode Akinwande) Date

Faculty Reader (University of Liverpool) Date

The University of Liverpool

2007

CERTIFICATION STATEMENT

I hereby certify that I am the author of this paper and that any assistance I receive in its preparation is fully acknowledged and disclosed herein. I have also cited any source from which I used data, ideas or words, either quoted directly or paraphrased. I certify that this paper was prepared by me especially for this purpose

James R Young

DEDICATION

This dissertation is dedicated to the memory of Private 19981 Isaac Young, The Border Regiment, who fell near Fricourt, The Somme in June 1916. The problem of dwindling fossil fuel supplies will bring challenges to societies the world over; sometimes it is pertinent to consider the costs of finding the wrong answer.

ACKNOWLEDGEMENTS

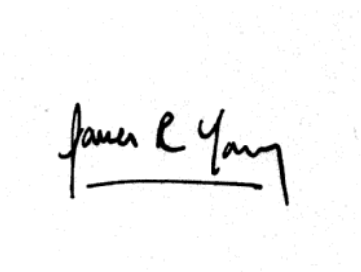
This dissertation would not have been accomplished without the help, advice and generosity of many people and organizations that have contributed to this project in a variety of ways. I would like to express my profound gratitude to :

Dr Bode Akinwande, my dissertation advisor, for his untiring professional support and guidance, positive expectation of the outcome and inspiration throughout the duration of the project.

Many individuals, some of whom have asked to remain anonymous, but particularly Mr Steve Foley and Mr Rob Willis for contributing their professional and personal experiences in their limited spare time, especially during the fieldwork.

The assistance of the lecturers, programme managers and support staff at the University of Liverpool is also acknowledged with grateful thanks.

Last but not least, I would like to thank my wife, Annalisa and my sons Joshua, Nathanial and Luke, for the sacrifices they have made over the past 3 years.



James Young.

Table of Contents

List of Figures :

Abbreviations and Acronyms

BCP	Business Continuity Planning
DR	Disaster Recovery
UK	United Kingdom
UPS	Uninterruptible Power Supply

ABSTRACT

AN EVALUATION OF THE READINESS OF UK COMPANIES FOR DISRUPTIONS IN ENERGY SUPPLY (1996 – 2006)

By

James R. Young

The UK faces long term challenges to the reliability of its energy supplies, arising from a combination of domestic resource depletion, subsequent dependence on eroding global raw fuel reserves, poor infrastructure investment and worsening weather. This study evaluates the readiness of UK companies for such disruption.

The literature suggests that the approach to business continuity planning is not taking account of these emergent risks and thus companies are unprepared. Selected UK businesses were asked for their views on business continuity planning. This information gathering comprised both qualitative and quantitative information obtained through questionnaire and interviews.

It was found that whilst most companies in the study had measures in place that would provide a degree of protection, there were shortfalls in their approach to risk assessment which meant emergent risks were not captured or mitigated against.

To alleviate these vulnerabilities, it is recommended that the UK government become more proactive in communicating emergent risks and that companies review their risk assessment approach and take appropriate action to ensure that protective measures are implemented and risks are regularly reviewed.

CHAPTER ONE

INTRODUCTION

1.1 Introduction

The UK is an island nation in the developed world. Historically, it has enjoyed the benefits of a geographically widespread and stable electricity transmission network, which, coupled with vast mineral resources within its own territorial waters, has contributed to high levels of energy availability and price stability. However, as these mineral resources become exhausted, the country will face increasing vulnerability to price fluctuation and global supply availability. Coupled with the predicted worsening of global weather patterns, there is a significant risk to UK businesses.

The area of study was found to be presently neglected, with, for example, most government initiatives focusing on the climate change agenda. Whilst specific study groups (such as the Association for the Study of Peak Oil, at Uppsala University, Sweden) are actively investigating macro impacts of hydro carbon depletion specifically, businesses need time to conduct risk assessment and initiate investment programmes to mitigate risks. Specific advice for businesses was not found to be forthcoming.

This study attempts to identify what shape these risks take, and the actions that UK businesses could take to minimize their vulnerability to electricity supply events that arise as a consequence. This chapter provides an overview of the research focus, sets problems to be investigated, details the objectives of the study and outlines the methodology that was used throughout it.

1.2 Background

The question of the sustainability of global energy supplies is one which, whilst undoubtedly being seriously considered by governments and energy companies, appears yet to capture the public imagination in any meaningful way. Whilst rising oil and gas prices are having an impact on UK consumers, most visibly through the high price of vehicle fuels, these price increases appear to be seen as a result of government financial policy, or short term supply disruption arising from war, natural events, or market forces.

In the academic world, the Peak Oil scenario, as it is known, is gaining credibility with a dedicated study group founded at Uppsala University in Sweden. Robelius (2007) claims that this peak may be reached as soon as 2008, and at the latest by 2018. Whilst the key focus of this Theory is the depletion of the world's oil reserves, the same scenario has been predicted for gas, the main fuel used in UK electricity generation [Wikipedia, nk]. Whilst gas is not expected to peak for another 60 years from a global standpoint [Bainerman, 2005] the problem in the UK is that it will shortly become reliant on gas imports. Hodgson (2004) is concerned that this reliance will expose the country to additional risks. Not only is gas more difficult to transport over long distances than oil, but much of the world's gas reserve lies in unstable regions – such as the former USSR and the Middle East [Alexander, 1997].

Both Hodgson and Mitchell (2000) are thus concerned that the gas supply to the UK could be disrupted by factors such as terrorism or war, or political disputes such as that seen between Russia and Ukraine in 2006 [BBC, 2006a]. Additionally, the 60 year forecast for global peak assumes that consumption will follow the model based on 1998 levels [Bainerman, 2005]. With massive economic growth in India and China this might be

questionable – the energy crisis felt by China in 2003 resulted in it importing 49% more energy than in the same period in 2002 [Cheng, 2004].

As the gap between available supplies and demand closes, the risk of disruption increases. This risk of disruption is compounded both by worsening weather effects attributed to global warming, structural problems in the distribution network [POST, 2001] and by the possibility of localized terrorist actions. Over the one year period that this research was being undertaken, the UK was hit by unprecedented flooding in Hull, Leeds, Sheffield and Carlisle [BBC 2007c]. Should London have been impacted in such a way, the effect on the British economy and the individual companies that make it up, would have been very significant.

Whilst many businesses have invested in backup electricity supply systems, it may be argued that this investment has been scaled based on a presumption of reliability and availability of energy based on the stability of the UK's energy supplies over the past 20 years. It was also perceived that the reason for these assumptions was grounded in best practice advice received by companies from specialists in the field, which typically recommend short term protection methods [Savage, 2003]. However, faced with the threat of sustained disruption brought about through failure of distribution networks, or by energy shortages, the decision process might be improved if businesses are to protect themselves adequately against outage.

1.3 Research Questions

Both Frost (1994) and Graydon (2005) state that business continuity investment decisions need to be based on credible risks. The literature review reveals that there may be a blind spot

in traditional thinking on energy supply risk and therefore the dissertation will try to address the following questions :

i) To what extent have the business continuity strategies of UK companies been influenced by this thinking ?

ii) What are the likely exposures that these companies would have in the event of serious supply disruptions and what are the strategies in place to mitigate them?; and

iii) What **other** policy recommendations could be advanced to reduce the risk faced by these individual companies?

1.4 Research Aims and Objectives

The specific aim of the project is to examine the most likely threats to energy supply, and identify any shortfalls in existing policies and strategies implemented by UK based companies. The scope was limited to companies operating computing / data centres in the UK; this limitation is discussed further in Chapter 6.

This aim was achieved through:

i) A review of publicly available government policies, directives and regulations in place where these describe actions to be taken when risks arise;

ii) Identification of any published risks relating to energy or primary fuel distribution in the UK;

iii) The evaluation of energy risk management practices within the British business community;

iv) The synthesis of opinions and experiences of contributors to the study, and

v) Recommendations on improvements to mitigate the risk faced by individual companies

1.5 Research Methodology

The study encompassed the collection of primary and secondary data from a number of sources. This information was sought through the following methods:

(i) Review of Available Literature (secondary data); comprising a review of academic literature, government policy documents and newspaper articles, the objective of this phase of the project was to identify and evaluate public domain information pertaining to energy policy in the UK, as well as best practice measures taken by individual companies

(ii) Collection of data through both interview survey questionnaire.

IT directors/managers were invited to contribute towards the study using an online questionnaire. Awareness of this questionnaire was raised through direct postal mailings to large companies, networking sites such as ecademy.com and LinkedIn, and the University of Liverpool's online classrooms. In this way, the response levels were improved from the relatively poor response received from direct mailings (see Chapter Four for further discussion of this point).

1.6 Layout of the Remaining Parts of the Study

To enable an effective evaluation of all the issues the remaining parts of the study are set out as follows.

Chapter Two provides a critical review of literature concerning current business practices and generic risk factors affecting companies today. It identifies new threats, attempts to assess how these threats would be mitigated by today's practices and identifies associated gaps in the risk planning process which became the key areas of focus for the research.

In Chapter Three, consideration is given to the nature of the UK electricity generation industry and the emergent risks that it faces. Additionally, the regulatory approach taken by government is considered, where this is relevant to the risk assessment process as it affects UK businesses.

The research methodology used in the study is described in Chapter Four, which also provides a justification for the approach and highlights limitations identified during the research process.

In Chapter Five, the results of fieldwork – comprising both questionnaire responses and interview feedback – are presented with interpretation of the results uncovered.

Chapter Six concludes the study, presenting a number of recommendations which may assist the individual firm in planning for emergent risks. This Chapter also discusses the limitations of the study, its contributions to existing knowledge and suggests areas for future research.

1.7 Conclusion

This Chapter has outlined the key hypothesis – that businesses face a number of emergent risks for which they are unprepared - and has presented a framework for the study that will allow conclusions to be drawn about the effectiveness of existing company strategies to mitigate risk. The problem and questions identified in this chapter were then developed through a review of extant literature, presented in Chapter 2.

CHAPTER TWO

REVIEW OF THE LITERATURE

2.1 Introduction

In 2004, The British Continuity Institute conducted a study examining attitudes towards business continuity in general [BCI, 2004]. The study found that the majority of UK companies have business continuity plans in place, but only 6% of companies considered that power failure would be a credible threat to their business within a 12 month horizon. Whilst the wording of the questions asked indicates an apparent failure on behalf of the authors to consider power failure as anything more than a localized event arising from infrastructure failure, rather than a wider and more sustained event, or a localized but recurring event, such as a rolling power outage, questions have to be asked about the validity of the views held by these companies. Power supply disruptions can be caused by any number of factors, most commonly infrastructure failure, extreme weather, deliberate act, and, more recently, disruption to raw fuel supplies.

Through a review of extant literature, this chapter presents evidence that not only are these risks very real, but that they are having an impact today, and that the impact and probability of such events occurring is increasing over time.

The literature also presents evidence of the existing practice followed by businesses with regard to business continuity planning, thus providing insights into the probable vulnerabilities that UK businesses will need to address. An understanding of these vulnerabilities, when combined with the risks inherent in the UK's energy industry that are

described in Chapter 3, is critical in defining possible actions to mitigate their impact. In the conclusion of this chapter, the key areas of concern are identified.

2.2 Analytical/Theoretical Framework for Analysing Energy Supply and Disruption

The key hypothesis investigated in Chapter Two is that businesses are not aware of, or responding to, the emergent risks uncovered in the literature. The approach taken synthesizes various types of literature in order to develop a picture. The framework for analysis comprised consideration at two levels – macro and micro :

At a macro level, consideration was given to literature relating to the risks facing the UK in relation to energy supply. The literature is useful in identifying the historical aspect – how and why risks have arisen – as well as in identifying and evaluating emergent risks. This process involved consideration of "natural" processes – such as evidence demonstrating worsening weather patterns and including consideration of hydro carbon depletion - as well as "artificial" risks created, for example, as a consequence of poor infrastructure investment or as the result of activities such as privatization. Consideration was also given to the UK government's approach to the issues of intervention (measures in place to address events after they arise) and regulation, as well as its approach to strategic investments that will guarantee the security of supply in the future.

The micro level focused on individual companies and aimed to assess the vulnerability that such companies had in relation to the issues addressed at the macro level. Once again, consideration was given to the historical aspect – specifically, what the traditional approach to business continuity entails - before considering more recent recommendations on how

businesses should protect themselves. The effectiveness of current business continuity measures, both in theory (recommendations) and in practice (as implemented) were considered. Businesses need a framework upon which to base their investment decisions and so the approach to risk assessment was evaluated to assess its effectiveness and recommendations with regard to cost benefit analysis were also sought.

2.3 Extant Literature on Energy Supply and Disruption

2.3.1 Hydro-carbon depletion

One of the key issues faced by industrial nations is how to meet their energy demands at a time when hydro-carbon fuel reserves are running low. Proponents of the Peak Oil Theory believe that the point at which maximum possible global oil production is exceeded by demand is close at hand, with estimates ranging from imminent to 20 years [Hirsch et al, (2005) pg 8] and around half of the contributors believing that it would happen by 2010. Hirsch et al point out that the market will signal the beginning of the crisis, through spiraling oil prices. Indeed, the general upward trend in oil prices over the past decade may be an indicator.

Whilst the effects of Peak Oil will be widely felt, it is a theory that largely sits outside of the scope of this study, because oil fired plant forms only a small part of most countries' electricity generating capacity. However, an extension of the same theory applies to gas – "Peak Gas" as it is known, is the point at which global gas production is eclipsed by demand. BP/Amoco, quoted in Bainerman (2005) estimate that world reserves will meet demand for another 60 years at 1998 consumption levels. The issue for gas, however, is that it is a very different fuel than oil. Whilst it burns cleaner, it is much more difficult to transport than oil

and consequently distribution tends to be regionalized. The US, for example, has to rely on self-sufficiency because of the problems with long distance transportation – whilst gas can be liquidized and carried in tankers, this is expensive [Bainerman, 2005].

This situation brings risks. Hodgson (2004) believes that supply could be threatened by "political instability in gas-producing nations", price could be affected by "risks associated with the supply and demand of gas" and the transportation problem (gas is more reliant on pipelines than oil) is also a cause for concern. Mitchell (2000) concurs with these points but argues that "the risk of politically motivated disruption now falls on exporters, not importers". This may be a shortsighted view – whilst countries such as Iran have seen export restrictions on oil, exporters themselves have also wielded the stick - in 2006 Russia cut supplies to Europe in a row over gas allegedly stolen by Ukraine, with France reporting that the volume of gas delivered had fallen by 40% [BBC, 2006a]. Mitchell goes on to describe regional war and the impact of domestic politics of major exporters as being other risks to supply. The Middle East is clearly the region most likely to be impacted by this, and as, in 1997, it held 32.4% of the world's proven gas reserves, this is clearly cause for concern [Alexander, 1997].

What form might an outage caused by a raw fuel shortage take ? In Chile, during the drought season of 1998/9, the country's hydroelectric plants were unable to meet demand and rolling blackouts were implemented in many cities. [El Mercurio, 1999 quoted in UCSD 1999]. In California, actions are also very clearly defined. Once electricity reserves fall below 7%, customers are alerted and asked to conserve energy. When levels drop below 5%, large customers who have voluntarily agreed to curtail power (in return for preferential pricing) are asked to do so. When levels drop below 1.5%, rolling blackouts are implemented [City of Concord, 2001].

The issue of gas security of supply is a critical one for the UK, which is heavily reliant on it for electricity generation. The specific challenges faced by the UK in this regard are discussed in Chapter 3.

2.3.2 Threats to electricity generation or transmission from severe weather and the impact of global warming

The traditional approach to the issue of continuity of power supply, as seen from the perspective of the business and outlined in Chapter 2, assumes that problems will be localized and short lived and this is undoubtedly true of most incidents – around 11% of incidents requiring the invocation of a business continuity plan in 2005 arose from local power issues [BCM,2006]. Whilst there have been major incidents affecting larger geographical areas, and these have been widely cited, they too have been mainly short lived – the Montreal power outage of 1989 [Odenwald, 2000], in which solar flare activity took down power for 5 hours, is one such example. Electricity generation and transmission are very susceptible to solar storms and whilst thus far, impacts have been minor, such storms follow an 11 year cycle, and the next cycle is predicted to be between 30% and 50% more violent than the current one [Salomone, 2006].

Terrestrial weather systems can also cause problems - the aftermath of the 2005 Gudrun Storm in Sweden provides evidence of what can happen, particularly in areas of poor infrastructure investment, with a power outage affecting some customers for up to seven weeks (Johannson et al, 2006), including a 2 week disruption to train services between two major cities. Neither was this storm unique. In France, a storm christened “Lothar” caused extensive damage to the French national grid, with 445,000 people being without power a week afterwards [EQE, nk]. In 1996, a US intertie (grid interconnection point) failed under

high temperatures, resulting in blackouts affecting nine states. In 1998, an ice storm caused prolonged blackouts in Canada. In 1998, one of 4 power cables feeding the central business district of Auckland, New Zealand, failed, probably due to high temperatures. The remaining cables became overloaded and failed, resulting a power blackout that lasted 5 weeks [Wikipedia, nk]. Many lessons can be drawn from Hurricane Katrina, which saw 11,000 utility poles being destroyed, $400 - $600m of damage to telecommunications infrastructure, and 3 million people being left without power or telecommunications [Sungard, 2006 pg 1].

2.3.3 Risks from Terrorism or Deliberate Disruption

Since the events of September 11th, 2001, public attention has been focused on the growing threat from terrorist organizations. Whilst there appears to be a shortage of credible literature relating to the threat of terrorist attack, it is clear that there are many opportunities for such an attack on raw fuel supply, power generation facilities, and electricity distribution systems.

Since September 11th, for example, there has been a significant increase in the number of recorded hacking attempts made against the control software used by North American power generation companies [PGJ, 2007]. This software, known as supervisory, control and data acquisition software (or SCADA), is in widespread use across all utility sectors, including electricity generation, oil and gas distribution and water supply. It has been identified as containing a number of vulnerabilities that could be exploited to bring down power generation in an entire region [Riptech, 2001]. In 2003, for example, a nuclear plant in Ohio was affected by a worm virus, which took a safety system offline for 5 hours [Poulson, 2003]. There is evidence that Al Queda in particular has an interest in attacks against utilities – a computer

found in Afghanistan was found to contain structural analysis of US dams and the number of internet searches for information related to SCADA systems has increased [Shea, 2003a].

Neither is the threat just a theoretical one – Shea (2003a) cites three specific attacks, where utilities including sewage treatment, telephony services and hydro-electricity generation were successfully compromised. Shea (2003b) also describes the anticipated impact of such attacks, when compared with similar accidental incidents – in summary, a SCADA attack, whilst it may have a widespread impact, is unlikely to have affect services for more than 1-2 days, a length of time that should sit within the capabilities of a traditional business continuity plan.

2.3.4 Business Continuity Practices

Business continuity, which is more popularly known as Disaster Recovery (DR) in technology circles, is a developing science and an expensive one. Winecki (2004) citing Metagroup (nk), projected that expenditure will increase from 4% to 7% of budgets between 2004 and 2006. He also cites evidence that, as of 2004, only 40% of Global 2000 businesses had comprehensive business continuity/DR plans in place and that this was expected to increase to 60% by 2005 (in fact, evidence uncovered during this research and described in Chapter 5 suggests that the figure is closer to 100% for the top 1000 FTSE businesses, but it is noted that "comprehensive" is a subjective term).

An individual company's approach to business continuity is influenced not only by budget, but also by industry. Winecki uses the example of the financial industry, which has "no choice but to build and maintain expensive recoverability architectures" and the logistics industry - for which such a model would be inappropriate because of the thin margins involved.

Traditionally, the DR function has largely been driven by IT staff, but this model is not sustainable because the purview of IT staff is limited and, typically, they do not understand business priorities, have problems obtaining funding and difficulties achieving proper engagement with other facets of the business [Winecki, 2004]. Business Continuity Plans increasingly face scrutiny from regulatory bodies, investors and others – one individual interviewed during this research cited difficulties obtaining business risk insurance because of concerns over the business continuity planning process. Winecki advises that to be effective, Business Continuity must evolve into a corporate level responsibility. He also advises that investments must be aligned with a company's risk aversion and made on the basis of considered risk assessment.

Wold and Shriver [1997] suggest that regardless of the prevention techniques employed, internal and external threats to the organization should be assessed and, whilst the precise nature of a disaster and its consequences may be difficult to predict, there is value in performing a comprehensive risk assessment of all perceived threats. They suggest that the relative probability of a disaster occurring should be assessed and should take account of issues arising from areas as diverse as specific geographical location, topography, proximity to major power sources, water and airports and the performance history of local utility companies. They propose that threats are classified as natural, technical or human threats and recommend that additional factors beyond the normal probability and impact scores are considered. For example, assigning a weight to the predictability of a disaster, the amount of forewarning and speed of onset might change the relative importance of a risk. Although they do not mention this point, the natural extension of this process would be to prioritise investments based on these weighted scores. Additionally, it might influence the approaches taken when an event occurs and the design of the mitigating solution. Traditional continuity planning, based as it is on the assumption of localized power outage, assumes that such an

outage would be sudden and without warning, and thus, for example, proximity to the affected site would be key to restoring service. However, in the case of outages arising from gas supply disruption, it is likely that forewarning would be available [Ofgem, 1999] and thus proximity might be less important – and in fact, may be less desirable.

The "Key Intelligence Questions and Topics" approach [Herring, 2001], more commonly used for market intelligence, might be a useful basis for the intelligence gathering which is the most critical element of this model. This approach will guide an evaluation of risks, and the measures that need to be put into place to address them. The KIQ/IT approach was originally developed by the US military as an effective approach to threat assessment and it has since been developed into a market intelligence tool [Herring, 2001]. A similar model was recommended by one of the interview participants and will address the concerns raised by two others. Consequently, it is an approach that has been proven both from a commercial and military threat perspective, with both perspectives being applicable to the scenarios discussed in this study. The answers to each question will drive the strategy that the company adopts in order to tackle emergent threats and, importantly, it enables the business to identify and monitor warning signs that might otherwise be overlooked. Warning signs are important – short horizon events such as hurricanes may only allow a business the opportunity to metaphorically batten down the hatches, but events taking place over a longer duration, such as fuel shortages, may be signaled earlier and will allow the business to make long-term strategic, as well as short-term tactical, decisions.

Ellison et al [1999] highlight the importance of the concept of "survivability" in risk assessment and disaster planning. Survivability, they argue, is the "capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents". In simple terms, it is the survival of the mission, rather than the system, that is key. This has

implications for continuity planning – organisations that have a clear understanding of the dependencies that exist within their own processes, and in particular those that have established and understood mechanisms to enable the business to continue to work towards its goals, even in the event of a catastrophic computer failure, are more likely to survive than those that do not. Continuity planning, therefore, is as much about ensuring that manual workaround processes are in place as it is about ensuring that computer systems remain available and it should start with the business process, rather than being built upwards from the technology platform.

Whilst such events are likely to remain rare in the UK, some relevant business continuity lessons can be learnt from Hurricane Katrina. During the hurricane, companies were impacted as much by displacement of staff and inability to communicate as they were by data centre damage [Sungard, 2006, pages 5-7] and thus businesses must think hard about how to address these issues when thinking in terms of severe weather or the implications of fuel supply shortages on transportation. With regard to systems themselves, however, some of the key lessons included the need to ensure that data is backed up to an offsite location a sufficient distance away to avoid impact during a regional disaster. It is also important to ensure that support contracts and inventories are up to date and available in the event of a disaster. The Sungard study suggests that businesses were unprepared for the severity of the storm but disappointingly, does not follow this thought process through – the experience is again suggestive that traditional risk assessment measures such as probability and impact should be complemented by speed of onset, forewarning, and duration of event as identified by Wold and Shriver (1997). The mitigation plans available to a business in a fuel shortage, where, one would assume, early warnings would be available, would then vary to the plans it might implement to address unforeseen events.

What measures can businesses usefully take to mitigate the effect of energy disruptions ? Perhaps disturbingly, there is little evidence that advice is changing in the face of emergent risks. The Department for Trade and Industry's factsheet on Business Continuity Management [DTI, nk] is suggestive that a failure would be a short term and localized event. Savage (2002) also specifically highlights power failure as a risk to business, stating that the main function of devices such as UPSs or generators is to ensure a "graceful" shutdown of services, thus preserving data integrity. However, such a solution is only of use if the services are either non-critical, or are available from another location. Passmore (2007), commenting on best practices in high availability storage networks, recommends the use of diversely routed power supplies from alternative power sources, or the use of UPS and generators. In the context of achieving high availability, his use of the word "or" is disconcerting. A widespread power supply failure is perfectly capable of suspending all external power, leaving the business that has not invested in generators quite literally in the dark. All interview respondents who responded to this point recommended the use of generators.

Mingay [2006] points out that IT has become so critical to most organizations that investment decisions will be driven by Recovery Point Objectives (RPOs) – the point at which data will be lost, ideally as close to zero hours as possible – and Recovery Time Objectives (RTOs). To achieve these targets, mid size businesses are mirroring the approach taken by large companies in investing in advanced technologies to counter the time problems associated with restoration of increasingly large databases. However, he also points out that effective business continuity depends as much on doing the basics right as it does on large scale investments. Specifically, he mentions that responsibility for a policy must be owned by an individual who oversees its execution and compliance. He also recommends that in order to maximize resources, businesses should focus on the most significant risks. However, he offers no guidance as to how businesses should handle low probability events that carry very

high impacts, such as those described in this research. This point was discussed with one interviewee, who noted that high impact, low probability events are difficult to effectively address.

2.3.5 Cost Benefits Analysis in Energy Supply and Disruption

Identifying the impact of low probability events may be easy, but what about the justification for investment in measures to prevent them – in particular, what are the positive benefits of such investments ? For many large companies, the ultimate step in cost/benefit analysis must be consideration of the impact on shareholder values, both in terms of expenditure required to address a risk, and the impact of the risk itself. Knight and Pretty [1997, cited in Graydon, 2005] evaluated the after affects of historical disasters on UK companies. Using the definition "recoverers" to describe companies who were successful in regaining shareholder value through market capitalization over the subsequent year, they found that for non-recoverers, the average loss was 15% of value 12 months later. Their conclusion was that the key difference between the two groups was lack of preparedness. Graydon concludes that there is "strong suggestion that BCP could be related to shareholder value, but in the absence of quantitative research one must be cautious to arrive at such a relationship" [Graydon, 2005 pg 12]. Tregaskes (2002) cites evidence that over 60% of companies that suffer a major disaster are no longer in business two years after the event and that of the 40% that remain in business "the majority" had disaster recovery plans. Graydon (2005) also suggests that there is a competitive advantage to business continuity that should be considered "those companies that can recover quickly….can steal a march on the competition".

Hales (2003) suggests that a number of factors influencing the cost/benefit decision have changed over the past 5 years. She cites September 11th, increased regulatory pressure, corporate governance, increasing dependencies on information availability and subsequent impacts on customer expectation and employee livelihoods as being reasons to invest. She suggests that the cost/benefit analysis should include consideration of the impact on four areas – a company's reputation, its brand, financial results and the costs that would be incurred as a consequence of failures. She also highlights the key point that without maintenance and governance, the benefits of investment will fade over time.

Tregaskes (2003) suggests that the business should first consider its objectives and the likely risks and impacts it faces – including the financial impact - before considering a range of options to mitigate these events. Nickolett (2006) expands on this by recommending that businesses begin by considering the financial implications of a disaster, including a cash estimate of lost sales and customers. Through consultation with the wider business, the technological solution selected will be a balance of cost and impaired functionality – "there is no point spending £100k on a solution for a problem that will only cost £35k" [Tregaskes, 2003]. This is a particular concern that would be addressed by consideration of shareholder value as recommended by Hales. Lanz (2002) agrees – in his survey of the business continuity strategies adopted by banks he recommends that because there are no set rules governing how cost/benefit conclusions should be drawn, courage is required to "select the strategy that provides the greatest enterprise value". He suggests that this might require unpalatable decisions to prioritise certain operations over others.

Cost Benefit Analysis is also important to governments. Triutomo (2005) speaking at the World Conference on Disaster Reduction said that the approach could strengthen the shift from reaction to prevention in local governments. He further stated that the "short planning

horizons" in public planning make it difficult to adopt risk management projects with longer term benefits realization. Mechler (2005) highlights that whilst cost benefit analysis is a tool for systematic and coherent decision making, because it is a monetary framework it is difficult to include non-monetary values. He cites Kofi Annan, who said that "the benefits are not tangible; they are the disasters that did NOT happen". Consequently, there is a disincentive to politicians to make investment decisions and a subsequent need for long term thinking. Like Lanz (2005), Mechler believes that the cost benefit analysis cycle will require decisions to be made based on the "most profitable option". Sugeng (2005) commenting on disaster planning in Indonesia, puts it more starkly "decision makers are more focused on new …projects with obvious benefits than preventing (disasters)" – a downside to democracy ?

A possible approach to addressing this shortfall is provided by Benson (2005) who recommends that guidelines for disaster prevention should be revised to ensure that economic activity sensitivity analysis be extended to specifically cover natural hazards, that these hazards should also be considered when considering the sustainability of projects. Additionally, the economic consequences of any change in vulnerability brought about through investment in mitigation . This latter point is important; reduced economic threat is a clear demonstration of benefit.

2.4 Unresolved Issues in the Literature

The literature provides an insight into the types of risk that businesses face, as well as the likely impact of these risks. It has demonstrated that, dependent on the nature of the disruption, the likely impact is either localized and sustained power outage, or the implementation of measures such as the rolling brownout, where businesses are exposed to regular and frequent power disruption for the duration of the supply crisis.

There are some important gaps in the approach taken by many businesses with regard to business continuity. Firstly, whilst proposing approaches to risk assessment, no evidence of the effectiveness of these approaches was found. This concern was noted by one BCP manager interviewed during the research, who was of the view that companies in his own expertise were “broad brushing” over areas that needed deeper consideration for lack of a documented approach. There is also a suggestion that cost benefits analysis could be better used to justify expenditure, both for the individual company and the government.

Little evidence was found that businesses are aware of the heightened risks to energy supply brought by issues related to global warming and hydrocarbon depletion, both of which have the potential to either themselves create, or exacerbate, an electricity supply crisis. However, the generic measures taken under the guise of business continuity planning within those companies may help to mitigate the impact that an event would have on business operations. Examples of such measures include the deployment of generators, consideration and testing of disaster recovery plans and a conscious delegation of the responsibility for business continuity planning. Additionally, there is evidence (from Hurricane Katrina, for example) that companies are not holistically considering end to end service availability in their continuity planning; ignoring key elements of a service, such as support contracts or telecommunications networks, leaves vulnerabilities unaddressed.

2.5 Conclusion

This chapter has presented an overview of emergent risks and provided an insight into the thinking regarding best practice for business continuity planning. The literature was then revisited to establish whether the nature of the infrastructure in the UK resulted in any specific vulnerabilities; this is discussed in Chapter 3.

CHAPTER THREE

UK Electricity Generation – An Overview of Industry, Regulation and Risk

3.1 Introduction

Whilst the challenges faced by UK businesses are in many ways similar to those of other countries, the geography and resources of the United Kingdom, the nature of the electricity generation industry and the role of government regulation are all worthy of evaluation in understanding some specific risks faced by UK companies.

This Chapter presents a critical review of academic and government publications in the public domain, providing an overview of the UK electricity generation industry and identifying the specific challenges it faces at a time when the country's gas supplies are running out, its nuclear generation capability is obsolete and climate change objectives are strongly influencing ongoing strategy. This evaluation is critical in completing the picture of the risks that UK businesses face in relation to energy supply.

3.2 Justification for Researching UK Power and Energy Supply and Disruption

The UK was chosen as the focus for this research for a number of reasons. Firstly, as a country in the developed world, it has very significant energy needs. However, its natural resources – particularly gas and oil – are in decline. The geography of the country means that some opportunities for alternative generation technologies – for example, hydro-electric power – are limited, whilst public distaste for nuclear power generation has resulted in very

limited investment in nuclear power over the past twenty years. Whilst the government is pushing investment in "green" technologies as part of its climate change agenda, there is public resistance which is delaying the implementation of such measures.

Additionally, there is evidence that the privatization of power assets has led to a situation where power transmission and generating networks have seen little investment and are poorly maintained. For example, the UK's gas transmission and storage facilities are significantly less robust than is normal in Europe.

The implication of these issues is that the UK – and its business community - may be more vulnerable to power outages in the future than companies in other European countries. Whilst this chapter looks at the issues from a UK risk perspective this is not to say that the chapter is not relevant to companies in other countries. As the UK was seen as a leader in the area of privatization, and many countries have followed the British model, it is likely that the challenges related to privatization will be experienced elsewhere.

3.3 Industry Information

The UK's electricity generation infrastructure comprises of three main stages. The first stage, Generation, is the generation of electricity from raw fuels such as gas, coal, nuclear power and, to an increasing extent, renewables. Transmission is the high voltage movement of electricity over long distances to distributors or high volume industrial customers. Distribution is the provision of electricity to customers through lower voltage networks [POST, 2001 pg 1]

The commercial model broadly follows this approach, with Generators being responsible for generation of power, Distributors being responsible for movement of this power from generator plant to end customer and Suppliers being responsible for the sale of the electricity to these end customers.

The national transmission network comprises 4 individual networks, the largest of which is owned by National Grid [POST, 2001 pg 2]. Interconnection between these networks means that the cheapest forms of generation can be used at all times, regardless of geographical location. This does, however, depend on the ability to swing capacity between generation methods, a point addressed later in this chapter. Transmission operators play a role in balancing generation and demand, thus ensuring the security of the network. They achieve this predominantly through energy trading [POST, 2001 pg 1]. This balancing is particularly important because the difference between generation capacity and demand varies from region to region within the UK. For example, in Scotland, generation capacity roughly balances local demand. In Southern England however, demand significantly outweighs generation capacity [see Figure 1, Appendix D].

UK electricity generation is predominantly fuelled by 3 sources – gas (39.93%), coal (33.08%) and nuclear power (19.26%) [Wikipedia, nk]. The proportion of electricity generation that is fuelled by coal continues to diminish, due to environmental concerns, and will account for only around 25% by 2010 [DTI 2002 quoted in Hodgson, 2004]. Oil plays a very small role in power generation.

With the present lack of significant investment in nuclear power, and the move away from coal, the demand for gas for electricity generation is likely to continue to rise. As the UK is therefore dependent on gas - and will remain so in the short to medium term - security of

supply must be seen as a key issue. In the US, this issue is also taken seriously – Darley (2004) suggests that behind the recent repealing of clean air bills may lie a concern over security of gas supply.

The validity of recommendations with regard to business continuity planning will be heavily influenced by the relevance of those recommendations with regard to a business' operating environment. In particular, the geographical location of a business will influence the decision making process – a company based in a low lying country such as Bangladesh would have very different considerations to one based in a mountainous region of the world.

Similarly, the electricity generation and distribution infrastructures vary between countries, and it is these same infrastructures upon which businesses are dependent. As will be seen, the UK faces a number of unique challenges which expose it to risks that are not faced by other countries. For example, the UK's gas storage facilities fall far short of what might be considered European standards. For this reason, an evaluation of the risks brought about by UK energy policy and regulation are important in identifying areas of special vulnerability for UK businesses.

3.4 The Role of Government (via Regulation and Intervention)

3.4.1 Regulation and Intervention

In the UK around two decades of stability in energy supply were threatened in 2005 when the UK government considered restricting supplies to chemical companies due to fears of increased domestic consumption [BBC, 2006b]. This was perhaps the first recent public

indication of a potential problem with the UK's energy supply although details were sparse as to how the government would react if this restriction did not resolve the problem.

In the UK, the Office of Gas and Electicity Markets (Ofgem) has responsibility for overseeing the electricity marketplace and setting priorities when events occur. Whilst some documents in the public domain [e.g; Ofgem, 1999] indicate that there is no consensus in place on the supply of gas to electricity companies in such situations – thereby suggesting that the demand for gas from domestic customers would take priority over industrial demand for electricity, the government has, in fact, established an "Electricity Supply Emergency Code" which details the approach that the UK government would take in the event of a supply emergency. The Code grants the Secretary of State the power to direct the operator of any conventionally fuelled (including nuclear) power station to operate, or not to operate, at specified levels of capacity (clearly a measure which would be used were a raw fuel shortage to occur). The Code also appears to address the ambiguity found in the Ofgem documentation – the objective of the Code is to "maintain an equitable distribution of available supplies to all consumers whilst protecting, as far as reasonably possible, supplies to industries and services on which the well-being of the nation particularly depends" [Department of Trade and Industry, 1999]. The Code allows the imposition of rolling blackouts (brownouts) or total power shutdowns, giving priority only to vital services – including telephony services - major food manufacturers and certain continuous process manufacturing companies. The Code enables enforcement through a whole series of Acts of Parliament - governing everything from supply of petroleum and other raw fuels through to display board advertising and street lighting.

The priority granted to businesses is worthy of note –it is entirely possible, for example, that during a severe blackout, residential homes would have power, telecommunications providers would have power, whereas an individual company data centre might not**.**

Industry regulation and intervention measures are facets of a government's role that are useful in the short term, but do not address the increasing pressures on the UK energy market, particularly considering the hydro-carbon depletion scenario. The role of government should extend beyond contingency planning to include policy setting and, if energy supplies are to be secured, Government must play a role in the strategic development of the UK's energy market. In addition to protecting existing supplies, in this area it has two roles – promotion of investment in new technologies, and promotion of energy efficiency. Although there is evidence that issues around security of supply are now coming to the fore in UK government thinking, the main driver towards sustainable (green) energy is still the climate change agenda. Whilst the issue is having an impact on sustainable energy, this is a very different issue to that of security of supply. If the objective is to reduce greenhouse gas emissions, fossil fuel power generation can be complemented by renewables in whatever proportion is required to attain the defined targets. However, if the objective is to ensure security of supply, the proportion of power generation that is sourced from renewables is likely to be greater to allow switching between technologies should one source of traditional raw fuel supply become restricted.

3.4.2 Long Term Strategy and Investment

According to Sinden [2006], investment in renewable energy will bring benefits to the UK in a number of ways. Firstly, it will provide it with an "independent, indigenous, source of energy". The nature of the fuel used (wind, water, sunlight) means that price security can be

attained – price is not linked to "volatile international fossil fuel markets". In Sinden's view, assuming gas prices do not increase, generating 20% of the UK's electricity from wind power or other renewables would result lower overall fuel costs "irrespective of the price of gas". In other words, although coverage in the press suggests that the UK government's focus appears to be more on the climate change agenda than hydro-carbon depletion, this focus will assist in securing energy supplies.

Grubb et al (nk) conducted an evaluation of the security of UK electricity generation, proposing two measures of security – robustness of supply of a raw fuel or energy source and the reliability of generation availability. For example, wind generation is less subject to market risks, and tends to be geographically diverse, hence it can be considered robust. However, the varying wind speeds encountered mean that it might fail the second test of reliability. Using this approach, and combining climate change driven scenarios published by the DTI (0% and 60% carbon reduction), the authors conclude that a move toward low carbon generation technologies will result in an increase in the security of electricity generation. This is largely because present generation capacity relies heavily on natural gas, whereas low carbon generation schemes generate electricity from a number of sources (wind, sun and water). A diverse source of fuel for generation that incorporates renewables means that there is less risk of disruption, as it is difficult to identify scenarios when all sources will be impacted by the same events. Additionally, the low generation capacity of individual components of a "green" scheme means that a high level of diversity is required within the system in order to smoothe out intermittencies within that system. In summarizing their work, the authors make a key point – "On the time-scales implicit in long-run energy projections, it is impossible to predict with confidence the specific sources of insecurity in energy systems. A more realistic approach is to seek systems that are diverse, and that are consequently more robust against a range of possible interruption." [Grubb et al 2, nk]. Sinden [2006] defines

security of supply as having a number of aspects – including physical security, price security and operational security. This is an important point – there is a tendency for businesses to consider security of supply to mean dependability. Sinden omits to point out that an unacceptably expensive supply could have as much of an impact on a business' ability to continue operations as its availability. Awerbuch (2003), however, points out that there is a "growing body of economic evidence that clearly indicates when fossil fuel prices rise or become more volatile, economies decline".

Awerbuch (2003) suggests that one reason that investment in renewable energy sources has been limited is due to the fact that fossil fuel outlays are underestimated, "making conventional generation appear falsely attractive". Decisions on investment are driven on a project cost per kilowatt hour (kWh) basis using traditional engineering economic modeling. This approach does not work for "capital intensive generating alternatives such as PV and wind" – technologies which have a high up front cost but very low ongoing costs – whereas for expense-intensive fossil fuel alternatives they are acceptable. Awerbuch highlights that the issue is one of risk evaluation – traditional analysis methods do not take financial risk into account and thus high risk issues – such as the high risk that fossil fuel prices will increase – are ignored. After the initial investment, renewable fuel sources are generally low risk – the cost of maintenance is unlikely to be as affected by market forces. The consequence is that the risk profile of conventional generation techniques is understated, making them look more attractive than renewable schemes. He draws a strong conclusion on the suitability of current calculation methods – "in spite of clear-cut evidence to the contrary, energy planners continue to use inappropriate cost models, conceived around the time of the Model-T Ford and long since discarded in other industries". Indeed, his own risk-adjusted estimates (see Appendix E) show that, with the exception of Solar Thermal Power, all forms of renewable energy generation carry significantly less risk than the conventional generation technologies.

A further constraint is political. Like any government, the fear of lost votes counterbalances any strong initiatives. Whilst Bjorkqvist (1996) cites Lovins (1990), who claimed that US electricity demand could be reduced by 75% and oil demand by 80% without increasing the cost of supply, the reality is that this would likely require harsh discipline on the part of the consumer – and few consumers are likely to respond positively, from an electoral standpoint, to such an approach. Perhaps unfortunately, the UK looks like it will surpass its Kyoto targets by 11.1%, meaning that some of the pressure on renewable energy investments is reduced [Defra, 2005] – avoiding harsh consumer-focused action is probably an easy option, therefore. However, consumer led efficiency is just one approach – Bjorkvist (1996) advocates the use of Demand Side Management, which rewards the energy generator for efficient use of raw fuels. In his study of two Swedish energy companies, he found that energy saving initiatives were only considered in the context of commercial reasonableness and suggests that the cost-benefit analysis should include the cost to the environment and society, in this way ensuring that companies invest in initiatives that might otherwise be ignored. Clearly, such a scenario is unlikely to be promoted by the energy companies themselves; this is a key role for Government.

3.5 Compelling Issues relating to UK Energy Supply

3.5.1 Dependency on Gas as the raw fuel source

Hodgson (2004) provides an overview of the challenges created by our dependency on gas. By 2020, he believes, natural gas will provide over two thirds of the UK's fuel consumption. Oil and Gas UK [2004], however, takes a slightly more pessimistic view, believing that gas production peaked in 2000, and that supplies from our own fields will only be able to meet

60% of demand by the end of the decade. Campbell, quoted in Bainerman (2005) believes the figure will be closer to 50%, with the UK swiftly becoming reliant on Norway and later, Russia, Central Asia, North Africa and the Middle East. The reason for the problem is twofold according to Bainerman – firstly, new discoveries have tailed off and secondly, clean air bills introduced by developed nations have driven the decommission of older, dirtier oil and coal fired generation capacity. In the decade between 1977 and 1987, 9,000 new gas fields were discovered. Between 1987 and 1997, only 2,500 were found.

Some studies observed that the UK is more susceptible to supply shortages than many European countries as it can presently stockpile only 13 days supply although plans are afoot to improve this [POST, 2004b]. According to Walter [2007], the UK stockpiles only 5% of its consumption, whereas other European net-importers stockpile up to 20%.

Hodgson also considers the impact of terrorist action or sabotage against the transportation infrastructure within a gas producer or transit nation, but neither he nor Mitchell consider the risk of terrorist action in the UK itself. As the UK has only two international gas pipelines as of 2004, this may be shortsighted [POST, 2004b].

3.5.2 Poor Infrastructure Investment

It may be tempting to assume that the UK's infrastructure is immune to such events. In fact, there is a culture of underinvestment both in capital projects and in maintenance and repair, with current capital expenditure needing to double even to meet existing demands [House of Commons, 2004]. Britain began privatizing its electricity generation capabilities in the early 1990s. The implied intention was to create a wholesale market as the main price-setting arena for electricity sales, creation of retail competition to allow consumers to choose

suppliers and to separate generation and retail supply. This latter point is important, since it implies that areas that would remain long term monopolies, such as the operation of the transmission networks, would be separated from market-driven areas. However, over time this distinction blurred, with companies such as Powergen and National Power supplying power to customers [Thomas, 2004] thus eroding real competition.

During the late 1990s, with wholesale prices very high, capacity investments were indeed made, but by 2002, with prices at "rock bottom levels" capacity was being mothballed. As a consequence, in 2003/04 National Grid issued a warning of a possible shortage of generation capacity for the coming winter and requested generators to bring plant back into service. Fortunately, due to this mothballed capacity, the problems were averted. However, as plants take 3 years from planning to output of power, there is a risk that future capacity signals will emerge too late, at worst leading to power blackouts [Thomas (2004) pg19]. This is a particular danger because nearly all the investment in generating plant since 1990 has resulted in poor rates of return, discouraging future investments. Around 40% of generation capacity is in the hands of bankrupt, or close to bankrupt, operators [Thomas et al, 2003]. The problem of investment is a particular one for expensive nuclear power generation. The UK presently has 19 nuclear reactors, located at just 10 sites within the United Kingdom, of which all but one are due to close by 2023 [AUA, 2007]. Indeed, most of the well known reactors, including Dungeness, Sellafield, Sizewell and Hinkley are already being decommissioned [BNG, nk]. With such a poor historical rate of return, the UK government will need to consider how to ensure that sufficient investment in nuclear power is made before the problems related to gas depletion begin to be felt.

Investment in generation capacity is just one issue. Thomas et al (2003) highlight that the rate of turnover in asset ownership in Britain is very high, with one example, the Eastern

distribution network, having had five owners in eight years. Whilst privatization was meant to bring efficiency, the incentive models put in place encourage network operators to scrimp on maintenance. Aside from profitability, the perceived risk of investment is discouraging - Standard and Poors, quoted in Thomas et al (2003) state that if companies are forced to invest in large infrastructure projects, their credit ratings will suffer as a consequence.

The 14th August USA blackout has been blamed on the stresses of trading electricity over long distance transmission lines, which were not designed for this purpose. Other issues identified included poor training, inadequate tree cutting, failure to maintain operations within safe limits, poor communication between systems and failure of computer systems [Thomas et al, 2003]. These same issues are being seen in the UK with poor training now endemic and a shift of employment from utilities to contractors, who have less incentive to train staff. The power outages in the eastern part of the UK in 2002 were attributed to a failure to carry out routine tree cutting work. (Thomas et al, 2003].

3.5.3 Specific Vulnerabilties to Terrorism or Deliberate Disruption

Whilst to date, the only impact to power generation or transmission in the UK has arisen from price rises which are themselves the result of raw fuel supply disruptions in the Middle East, it is certainly plausible that terrorist actions could be directed against electricity generation or distribution in the mainland UK. The UK's parliament was sufficiently concerned by the threat to publish a document detailing the threat to nuclear power generation, particularly from aircraft [POST, 2004]. However, the focus of this document is, as might be expected, on public safety rather than impact on power generation. A September 11 style attack on a nuclear power station might not result in release of radiation, but it would likely have a severely detrimental impact on that plant's generation capabilities. As the

number of plants reduces, the potential for serious disruption increases – an attack of a similar size to the September 11 strikes would have a significant impact on generation capabilities. Additionally, nuclear power offers an element of swing capacity – should another primary fuel source be impaired, a percentage of the nation's needs could be provided by nuclear power. Thanks to the decommissioning programme, this is no longer the case.

Nor is gas supply itself invulnerable to attack. Work is ongoing to increase the number of international pipelines bringing gas into Britain, however Britain's status as an island nation means that there will always be vulnerability here. The vulnerability does not apply solely to international transportation of raw fuel - Transco's schematic of the UK distribution network (see Appendix E) would appear to indicate a number of potential points of failure or attack, particularly in the high pressure transmission networks in the north of the country.

In summary, there are a number of vulnerabilities that could be exploited by terrorist groups. An attack on control system software (as described in paragraph 2.3.2) would have a localized effect, and even in the worst scenarios, a widespread effect that would be short term (1 – 2 days) in duration. A well-researched and coordinated physical attack, perhaps targeting both gas supply and nuclear power generation, might have a more sustained and longer term impact. As such an attack has not taken place to date, it is difficult to assess the likely effect in terms of duration or impact. However, the after effects of a terrorist attack might be similar to those seen following severe weather.

3.6 Conclusion

This chapter has presented a case study of UK Power and Energy supply and disruption with supporting published sources, as it relates to specific vulnerabilities arising from the nature of the electricity generation and transmission supply infrastructure in the UK and its dependence on gas. It suggests that the UK faces difficulties arising from a culture of poor investment in its generating capacity and transmission infrastructure, a concern that it seems must go unaddressed without government intervention, because of the poor financial health of many of the companies involved. This culture means that the UK infrastructure may not be robust enough to withstand deliberate damage or that arising from worsening weather patterns. This lack of investment extends to new generation capacity, which would alleviate some of the risks associated with the UK's dependence on gas. Evidence was also uncovered that the UK government is active in developing green energy strategies, driven predominantly by the climate change agenda, but with some evidence that the issues of security of supply are being taken into account. However, effective measures to improve generator efficiency and reduce consumer demand might be being impaired as a result of the country surpassing its Kyoto protocol targets.

This evidence, combined with the evidence relating to generic risks and best practice outlined in Chapter Two, suggests that there is a need for companies to ensure that their business continuity practices are robust enough to address the kind of issues that might arise as a consequence of these factors. The effectiveness of the measures taken is evaluated in Chapter Five. The outcome of the literature review is suggestive that the traditional view of energy risk - and ways of mitigating it - has not changed significantly, despite the perceived increase in risk factors affecting the availability of power.

CHAPTER 4: RESEARCH METHODOLOGY

4.1 Introduction

This chapter presents the research methodology adopted and presents justification for the the various approaches that were taken. It also discusses a number of limitations that were uncovered during the research programme, the majority of which arose due to confidentiality concerns.

4.2 Justification for using Qualitative and Quantitative Research Methods

In defining an approach for this research, it was felt necessary to adopt a dual approach to gathering primary data. Firstly, in order to gain an understanding of whether the key hypothesis was valid, a quantitative method was needed. This was felt necessary because other approaches – such as approaching a small group of individuals, or indeed conducting a single case study – might result in a viewpoint being identified that was not widespread across an industry. It was hoped that the use of a survey would offer the opportunity to gather opinions from a wide number of individuals, hopefully from different industries, thus allowing useful comparisons to be made about the relative vulnerability of each industry.

However, in understanding what views are held on the importance of energy risk considerations in a business continuity strategy, it is also necessary to understand why these views are held. Qualitative data capture “qualities or characteristics” about a subject (for example, their opinions [Rumsey, (2003), pg 98] and were useful in this context. For this reason, a smaller group of 15 individuals were approached and asked to participate in an interview; 5 individuals accepted this invitation.

4.3 Data Collection Methods

4.3.1 Secondary Data

Secondary data is data that is already in existence, often arising from previous research. This can be in a quantitative or qualitative form although in this study, secondary data was largely qualitative. The approach included a review of academic literature as well as articles from industry journals, company white papers and news reports.

4.3.2 Primary Data Collection (via Questionnaire Survey and Interviews)

Primary data is data that is gathered by the researcher for a specific purpose. The study made extensive use of primary data, both in qualitative and quantitative form, and arising from the conduct of interviews and survey questionnaires.

Questionnaire Survey: A sample population of 250 companies was selected. This sample was drawn from the 1000 largest FTSE companies and comprised the top 250 companies in terms of employee numbers. These criteria were selected as it was felt that some companies might have very large market capitalisation but small commercial operations. It was felt that companies with large numbers of employees would be more likely to have significant computing operations and that a sample size of 250 would be acceptable. A commercial database containing the names of IT Directors (or similar titles) was purchased and information from this database used to formulate personalized surveys which were mailed to the target population. The survey was pilot tested with the researcher's work colleagues prior to issuance particularly because, for forms of data gathering administered impersonally, there is risk of misunderstanding. The survey was opened on 15th March 2007 and closed on 12th April 2007.

In order to mitigate the known problems with response rates, the researcher also used an online survey and requested input from IT professionals using various business networking sites (predominantly LinkedIn.com and eCademy.com). A total of 46 completed responses were received via this medium.

Interview Approach: Interviewees were selected from those who had completed the survey questionnaire; clearly the response rate from those who had not done so would be much lower. Whilst it was hoped that all interviews could be conducted face to face, in reality only one took place in this manner. The interview process took place between April 2007 and July 2007, a timescale that was driven by the availability of those who agreed to take part. The data gathered from this process were useful in expanding upon the qualitative data obtained from the survey, and offered a much more detailed understanding of the processes and investments made by the associated companies and, importantly, what those within the companies thought both of their company's approach and of the risks described in this research. A total of fifteen people were approached and asked to participate. Due to confidentiality concerns, six declined, four did not respond and only five were able to contribute.

4.4 Ethical Considerations

The key ethical issue in this study was that of confidentiality. Increasingly, companies are penalized for misdemeanours by impact on stock price and the likely impact on an individual were such an event to occur would be significant. For this reason, all feedback, whether from surveys or interviews, was stripped of identifying factors and interviewees and survey respondents were made aware of this fact. Despite this, the number of responses was low -

and a number of uncompleted surveys were received with explanations that participation was not possible due to concerns over this issue. It was also important that interactions between the researcher and individual interview participants did not reveal information about actions taken by other companies, particularly where there was a risk that the names of those other companies could be inferred from the conversation.

4.5 Data Analysis

The data collected was analyzed to identify where cases of respondent bias might have occurred. In particular, the data collected from the online survey process was considered. It was found that a significant number of entries had to be removed from the sample as they did were of limited usefulness. It was felt that some respondents (for example other MBA or technology students approached via the University of Liverpool) had responded to the survey out of a sense of obligation. In addition, some companies comprised only 1 or 2 employees – clearly not an environment where significant investment in data centre infrastructure would be considered. Although not a flawless approach, it was concluded that two survey questions could be used as an indicator of whether a respondent could be considered authoritative in his or her organisation – specifically, a respondent with authority would likely know whether the organisation had an individual tasked with looking at business continuity. Likewise, the respondent would also be expected to know whether a business continuity strategy existed. Where a respondent had answered “Don’t know” to either of these questions, the results were removed from the sample. Any surveys where large sections had been left incomplete were also removed.

Some respondents had provided information on companies that were outside of the research scope due to their geographical location; these were removed from the sample.

This exercise resulted in the removal of 21 records, leaving a sample size of 36, including all 12 of the completed postal surveys. It has to be said that this response rate is lower than would normally be acceptable [Rumsey, (2003) pg 270]

None of the data removed from the survey sample were discarded – data provided by non-authoritative respondents was used to provide an effective comparison between the views of people who were essentially technical laymen, and those who were more obviously tasked with business continuity. In a similar way, information pertaining to companies based in other countries was also retained for comparative purposes.

4.6 Problems with the research approach

Initial response to the survey was predictably low, and so each target respondent received either an email or telephone call to follow up. In total, of 250 surveys mailed out, just 12 completed surveys were received within the time allowed (21 days). An additional 6 respondents stated that they were unable to assist with the research as the questions were considered to be commercially sensitive. Unfortunately, the low response rate is probably indeed indicative of the sensitivity of the information – there is an increasing focus on business continuity and security of computer systems in general, and an admission that a strategy is flawed might well lead to an impact on share price. It is noteworthy that all of the completed questionnaires received were from companies who clearly take business continuity very seriously – and for reasons described in Rumsey (2003, pg 89) it would likewise be dangerous to assume that the sample is representative.

4.7 Conclusion

This chapter has discussed the research approach, provided justification for the methods used and has provided an insight into where limitations were encountered. The next chapter presents the results of the research and offers analysis and interpretation of these results.

CHAPTER FIVE

PRESENTATION AND ANALYSIS OF RESULTS

5.1 Introduction

This chapter presents the findings of the survey and highlights areas of concern in the responses received that may indicate vulnerability to the events described in the literature. The hypothesis – that companies are not aware of, and not responding to, the threat posed by hydrocarbon depletion and associated issues – can be answered at a number of levels. For a company to mitigate a risk, it must first be aware of it. The data was therefore examined to identify whether this awareness exists. However, this is a simplistic evaluation because the impact of supply shortages, in the short term, is exactly the kind of risk that a business traditionally might mitigate against through its business continuity planning process. Comparisons were therefore drawn between companies who show an awareness of the issue, and those that do not, in terms of their approach to business continuity. In this manner, current practice can be identified and its effectiveness evaluated.

The presentation of results follows this format – firstly, in section 5.2, a simplistic analysis of awareness, followed by a more detailed analysis of the business continuity measures taken by all companies, to establish (i) whether companies who show an awareness of hydro-carbon depletion are taking effective measures to address it and (ii) whether the measures taken by all companies will be effective were such an event to occur.

5.2 Are Companies aware of Issues around Hydro-carbon depletion ?

Awareness of the Peak Oil Theory was used as a baseline indicator of awareness. The Peak Oil Theory deals with oil depletion and therefore, in terms of electricity production, is of lesser interest to the UK, which generates most of its electricity from gas. However, Peak Oil is becoming widely publicized – an internet search for this phrase using Google turned up 1.26 million references, whereas a search for "hydrocarbon depletion" and "fossil fuel depletion" brought up 22,000 and 29,000 references respectively.

Of 36 respondents, only one claimed to be "very familiar" with the Peak Oil theory, whereas 29 (80%) stated that they had no awareness of it. When compared with the data removed from the sample for the reasons described in Chapter 4, there was found to be a greater awareness in this latter group (30% aware). Whilst these data must be treated with caution given the size of the sample and concerns over data quality, they may imply that awareness is greater at lower echelons of the organization. In fact, when interviewees were questioned further on the subject, all of those who admitted an awareness of Peak Oil said that it had no present impact on continuity planning. On this basis alone, the hypothesis that companies are not aware of the threat from hydro-carbon depletion – can be considered proven. However, as outlined earlier in the research, Peak Oil was used as baseline to measure awareness; it is not in itself a threat to UK power generation because gas is the predominant raw fuel. Awareness of the importance that raw fuels play in the electricity generation process is important in facilitating an informed approach to risk assessment. When questioned on this point, only 17% of respondents in the sample correctly identified gas as being the key primary fuel; once again, the awareness was slightly higher at 25% from responses in the data that was excluded from the sample.

Respondents were asked where the UK obtains most of its gas from. Exactly 75% of respondents believed that the UK is dependent only on either domestic supplies, or supplies from Norway, a politically stable country with close links to Britain. Whilst this indeed true today [Hodgson, 2004], Oil & Gas UK [2004] believe that the UK will become reliant on other large gas producers such as Algeria and the former Soviet Union. This understanding is key to understanding threats to supply. When asked when the UK's position as net exporter would end, respondents were in accord with the literature, with almost 89% believing that our position as a net importer will end within 10 years, and 55% believing that it will end within five.

As our dependency on foreign gas imports increases, so does our susceptibility to supply problems arising from issues as varied as production curtailments (such as those seen in the wake of Hurricane Katrina [DOI, 2005]) and political instability. As an indicator of how respondents view such risks, views were solicited on the risk to the UK of the recent dispute between Russia and Georgia. A total of 27 respondents rated this as a "Medium" or higher risk, with 4 believing this to be a very high risk. However, of the 4 respondents rating this risk as "Very High", only 1 had correctly identified gas as the key UK raw fuel. This is perhaps reflective of the wording of the question – 27 respondents felt that electricity generation could be affected, but no estimate of the impact was requested. However, it also suggests that gas is not seen as being of critical importance to the UK.

It is therefore clear that the majority of businesses are presently unable to make a meaningful assessment of risk as it pertains to raw fuel supply; the connection between publicized gas supply events and possible impact on electricity generation is not being made.

Additionally, the majority of respondents do not seem to be aware of the more general issue of fossil fuel depletion.

5.3 How do companies rate other risks to electricity supply ?

It was felt important to assess how companies view risk from several key factors. The events considered in this section reflect those which businesses typically attempt to cater for in their business continuity plans and are important because the impact of such an event, and the business response to it, might parallel the impact of an event triggered by a supply shortage. Only around 20% of respondents saw a terrorist strike as a high risk in the next 5 years. Five of these respondents were headquartered in the UK, but interestingly none of these headquarters buildings were based in London, which might be considered the prime target for a terrorist attack. At 20%, this percentage is lower than found by the BCM (2004, quoted in Graydon, 2005) and suggest that the fear of terrorism is diminishing over time, a finding which backs up the findings of D'Antonio (2003 quoted in Graydon, 2005), who suggests that this lessening interest may mean that lessons have not been learned.

Questioned on the threat posed by worsening weather, respondents felt that this was very similar to that of terrorism, although at 22.2%, slightly more respondents believed that weather posed a significant threat. It seems likely that the priority assigned to weather events will continue to rise. When questioned about whether a national grid failure could cause a significant issue, only 13.9% believed that to be the case, which is perhaps surprising given the concerns raised in the literature.

5.4 Approach to Business Continuity

Understanding how a business approaches the issue of business continuity is important as it allows assessment of vulnerability to a supply shortage. A company that actively addresses issues around business continuity is more likely to have effective countermeasures in place than one that does not. Businesses were first asked to comment on whether they had an individual responsible for business continuity. Of 36 responses, 28 responded positively, with one postal respondent commenting that this responsibility was allocated to a team, rather than an individual. It is therefore possible that a larger number of companies have taken the step of assigning responsibility to a team or individual than would appear to be the case from the responses. Certainly, this would appear to be backed up by the fact that all 36 respondents claimed to have a business continuity plan.

This result is rather more favourable than was found in the 2006 survey conducted by the Chartered Management Institute, where only 48% of respondents admitted to having a business continuity plan (Woodman, 2007a), however this discrepancy probably arises from the nature of the companies being surveyed (the CMI survey covered companies of all sizes) and the probable impact of confidentiality concerns - highlighted earlier in this document - which resulted in a lower than expected rate of return on postal surveys.

An effective business continuity plan (BCP), must, as its name suggests, address all aspects of continuity within the business and not just focus on data centre availability. Responses confirmed that, in 80% of cases, the BCP did indeed address all aspects of the business. Of 5 respondents who agree to participate in an interview, all confirmed that BCP was being treated at this level, although most still felt that the bulk of responsibility fell upon

the IT department. One respondent went further, claiming that the approach of delegating responsibility meant that there was no real interest in the detail at corporate level – only an assurance that a plan was in place was sought.

Regardless of what elements of the business are covered, such a plan will only be effective if it is regularly tested. Given the potential disruption that would be caused to a FTSE company if a simulated power failure did not go as planned, it is perhaps unsurprising that only a small number of companies (8.3%) test their power failure capabilities more than once per quarter. In total, 26 out of 36 (or 72%) companies perform tests at least once every two years, rising to 82% if the "don't know" responses are apportioned across the range of answers. If power failure tests can be considered to be part of an organizational business continuity test, then the results are in line with Woodman (2007b) who found that around 50% of companies test their plans at least once per year. This result implies that many companies are carrying the risk that their plans will not work when needed.

Interestingly, the adjusted percentage of companies with plans that test power at least once every two years matches with the number of companies who have a business-wide BCP in place, and may suggest that the business buy-in that comes as part of a business-wide BCP planning exercise provides support for activities as potentially business disrupting as power failure testing. The reliance that IT departments have upon the business in allowing testing to take place was confirmed by several respondents.

On the face of it, then, the businesses that responded to the survey are taking business continuity relatively seriously and, based on comparison with the work done by the Chartered Management Institute, as well as, or better than, other UK companies. However, the key question is perhaps whether the business continuity plans that they have in place will actually

be effective should an incident occur.

5.5 Sources of Advice

It is common practice for companies to seek external expertise for areas outside of their core business. In the case of business continuity, the assumption is that external consultants will have a greater depth of knowledge about risks to the business. It was felt important to investigate this point because, if emergent risks such as those discussed in this paper are not being considered by specialist advisors, there is little hope that companies will be aware of, or able to react to, such risks. Just under half of respondents (17 / 47%) had worked with an external consultant in the definition of the business continuity plan or data centre design and of these 17, only 6 were advised to look at upstream supply risks or possible national-level disruptions. However, whilst these issues were discussed, it is not clear from the responses to the survey whether recommendations were made on these points. One company was advised to site its data centre away from major sites such as airports, but it is not clear from the data what the reasoning for this recommendation was – although we can assume it was to address concerns over accident or terrorist strike. In summary, whilst nearly half of companies in the survey sought external advice from specialist providers, there is little evidence that these specialist providers are themselves aware – or at least concerned by – any of the emerging risks highlighted in this study, evidence that was also missing from the literature.

In addition to the use of consultants, companies might also choose to seek advice from their power supplier in relation to their DR strategy or data centre design. Survey respondents were asked to confirm whether, during their data centre design process, any consultation with their power provider took place. A total of 28 (78%) respondents did undertake consultation, however, when the reason for consultation was provided, only 12 (33%) stated that this was to

evaluate resilience in the supplier's own network. One respondent commented that the supplier was trusted to take necessary steps to ensure resilience in their own infrastructure, because "that's what SLAs are for". This may be true, but SLAs (Service Level Agreements) are built around risk, and may simply indicate that the supplier is either unaware, or unconcerned, by the risk might be expected, or that such a risk is considered acceptable by the provider. With a reluctance to include consequential damages clauses in supply contracts, a question must be asked – who does such an SLA really protect and can the business accept such a risk at face value ? The 12 respondents who did consult also used the consultation to establish whether local power diversity was in place, as well as to ascertain whether sufficient local capacity existed. Of those companies that did not investigate upstream continuity, only 3 were concerned with local diversity, 6 held no discussions whatsoever and 11 were unable to comment. With only 33% of total respondents actively investigating the issue, this response is another clear indicator that issues beyond local diversity are not being considered by the majority of businesses.

Although newer server technologies are bringing down per-device power consumption, the general trend of data centre power consumption is upwards. It is therefore important that growth implications are understood and regular reviews held with suppliers. Only 52.8% of respondents reviewed power requirements in advance. Respondents were asked how often they compared their growth forecasts with the total capacity available from suppliers. One interviewee said that this had been a problem in the past and had resulted in a serious outage; the company was more rigorous in its approach as a consequence. Respondents were also asked how often capacity was reviewed with suppliers - only 13.9% reviewed this capacity on a quarterly, or more frequent basis. Considering the length of time a power upgrade can take, this is concerning. The danger is that if one power feed is lost, the remaining feeds could become overloaded.

5.6 Data Centre Design and the risks of a power supply outage

To recap, the literature demonstrates that the type of disruption that might arise from a global warming or fossil fuel depletion-driven supply event is slightly different in nature to what might be expected from a localized power supply failure – this local event being the type of event catered for in traditional business continuity plans. UK policy, and experience from countries such as Chile or Sweden, that have experienced severe raw fuel supply curtailments or severe weather, demonstrate that the duration of the event is likely to be characterized either by a total outage of long duration, or a long period of regular planned disruption (brown-outs). In such situations, it is not likely that traditional short-term measures such as the use of UPS or other battery backups will be adequate and companies using these as a primary defence mechanism would be unable to sustain normal operations. Hence, an assessment of the effectiveness of data centre design is useful in pinpointing specific vulnerabilities.

Respondents were asked to comment on some issues related to data centre design that might have an effect upon susceptibility of that data centre to power failures. Firstly, the number of incoming power feeds is important as it is an indicator of susceptibility to localized power failures (perhaps arising from weather or deliberate act such as terrorism). It is common for power feeds to be routed from different electricity substations, thus reducing vulnerability. As might be expected from companies as large as those in the survey, 94.4% of respondents had at least two power feeds coming into their data centres. This indicates that localized power failures affecting only one substation are unlikely to have a material impact. More widespread failures can be mitigated against using generators. A total of 77.8% of respondents had installed a generator. However, best practice suggests that to be resilient, "N-1" resiliency (ie, every component must have a backup) should be considered [House of

Commons, 2004b para 1]. One interviewee commented that a reason for using co-location services was because such resilience levels were attainable. Respondents were therefore asked whether additional generators were available to support this configuration – a total of 52.8% of companies equipped with generators had opted for additional backup in the form of a spare generator. This number rises to 65% if the companies without a generator are removed from the results.

In theory, a company that is able to generate power independently should be able to continue the data centre operations (defined as within the scope of this study) indefinitely. However, this would require an available supply of fuel. A concern raised by an interview participant was that this was a dangerous assumption given that, during the UK fuel protests of 2000 [BBC, 2007], disruption to fuel deliveries meant that petrol stations quickly ran dry and the government commandeered available petrol and diesel supplies for the use of essential users (such as medical and police personnel). Whilst gas, being predominantly used by residential users for heating, is unlikely to be substituted by petrol or diesel by those same users, there is at least a possibility that restrictions on purchase would be put into place – for example, essential users such as hospitals might be granted priority if the disruption was severe enough that they, too, were to become reliant on generator power. An outage of long duration, or a series of brown-outs, would certainly result in a heavy demand for diesel from other companies – a presumption that generator fuel would be easily available might therefore not be appropriate. Whilst no data was uncovered during the research, the demand for diesel fuel that would arise should a London-wide power outage occur would be very significant. When asked what volume of fuel they held at their site, a large number of respondents (30.6%) were unaware of the volumes held. Given the seniority of those canvassed in the survey, this may be a concern and may reflect the presumption that fuel will be readily available – alternatively it may simply be that such a responsibility and awareness is

delegated. Only 5.6% of companies held more than 2 weeks of fuel on site, which would equip them for a sustained outage or a series of brown-outs. If an outage were to last for more than 48 hours, 6 companies would lose power, rising to 10 (or 27.8%) after 1 week. Considering that of a sample of 36, 7 companies had declared, in previous questions, that they had no generator, and 11 were unsure of the fuel provisions made, this is a very high number. If the sample data holds true across the general UK population, less than 6% of companies could sustain data centre operations for more than two weeks, assuming fuel replenishment was not available.

On a more positive note, when asked whether preferential fuel agreements were in place, 19% of total respondents (or 24% of those with generators) confirmed that they had established such agreements.

A properly equipped data centre can survive indefinitely, assuming fuel for generators is available. However, if it is to support ongoing business operations, it needs a number of external interfaces. The scope of this research excluded any evaluation of the readiness of company processes and personnel, outside of those involved in maintaining the data centre, for such events. However, the level to which companies had considered the most key component – telecommunications – was evaluated. The response to this question was concerning. A total of 21 respondents (58%) were unaware of how long their local telecommunications provider could continue to provide service during a power outage. An additional 5 believed that services would fail after 24 hours, rising to 8 after 48 hours. Of the 5 respondents who expected telecommunication services to fail after 24 hours, 3 also stated that their data centre could only provide critical services for this period, indicating that, despite measures put into place locally, service availability was being driven by the capabilities of the telephone operator. One respondent, for example, stockpiled enough fuel

for 2 weeks, but could only sustain services for 24 hours, meaning that the investment in generating capacity was effectively wasted if connectivity to the outside world were required.

Network resiliency can change over time, partly as a result of changes made further down the supply chain. Respondents were asked how often they reviewed the resiliency of their network with their data provider. Of those that were aware of the frequency of such reviews, responses were fairly evenly split between monthly, quarterly and yearly reviews, and those that conduct no reviews at all. The 19% of respondents who do not perform any reviews are solely reliant on pro-active information coming from their provider. However, with SLAs that protect this provider as much as the customer, it may not be safe to assume that the required monitoring has any level of priority.

5.7 Buying Time – Options available to companies in the event of a failure

The events considered in this research – specifically, fuel shortages and electricity disruption caused by terrorism or weather – whilst having a similar effect, differ in terms of early symptoms. For an outage driven by a disruption to raw fuel supplies, it is likely that advance notice would be available and in such circumstances, transferring operations to another data centre might be considered. A total of two companies (6%) had no ability to transfer services between data centres. Eight companies (22%) had the ability to transfer to a data centre outside of the UK, which might be considered optimal as it would be unusual for another country to be afflicted with the same issues at the same time. The remaining 26 (72.2%) had the ability to relocate services to another location within the UK. This option would be acceptable were the event to be regional (for example, the flooding that occurred in Sheffield in 2007 [BBC, 2007b]) but would do little to address an event with wider impact. Additionally, there is anecdotal evidence that many City based companies prefer to build

backup data centres within the M25. These could therefore still be affected by events occurring in the City itself – "The high concentration of data centres within the M25 is itself a serious threat to the integrity of a business's data security strategy" [Smith, (2005) quoted in Continuity Central (2005)].Interview participants felt that a secondary data centre, if affordable, would be a good strategy.

A decision to switch services between data centres would be a difficult one to take in a situation where no impact has yet been experienced, because such an activity would itself, in most cases, carry a high cost in terms of disruption to business as usual activities and displacement of staff. Nevertheless, it is an option that would bring peace of mind were it to be something that could be achieved quickly. When questioned on this point, the majority of respondents (80.5%) believed that such a transfer could take place within 48 hours. Only 11% of total respondents would require a longer period of time. Nine respondents (25%) claimed to be able to affect a transfer in less than one hour. Whilst modern technologies would not in themselves be a bar to such a target, it is aggressive and achievement in practice is harder to achieve than on paper. All 9 of these companies were approached by email for further information on this point; only two responses were received at the time of writing, both felt unable to comment further.

It is also noteworthy that 3 respondents claimed that the process would either take longer, or that no facility existed. In the previous question (which related to availability of such facilities) only 2 respondents selected this answer. This discrepancy may be explained by the fact that some companies do have secondary data centres but are unable to easily transfer services between them.

Depending on the scenario, and the warning signals available, companies with the ability to swiftly move facilities have a clear advantage over those that do not. However, this advantage is lost if warning signs are ignored or decisions are delayed. A proposed method of addressing this problem is presented later in this document.

5.8 Conclusion

This chapter presented the results of the survey, where appropriate, compared this with findings from other research and opinions of respondents who agreed to be interviewed, and highlighted areas of concern. In the next chapter, the specific conclusions from the research are laid out, along with appropriate recommendations to address the areas of concern.

CHAPTER SIX – CONCLUSION AND RECOMMENDATIONS

6.1 Introduction

This chapter documents the conclusions drawn from this study, whilst providing some recommendations that businesses might choose to follow to mitigate some of the risks identified during the research process. It outlines a modification to existing risk assessment models, and concludes with a recommendation for further research.

6.2 General Conclusion

This study investigates the level of vulnerability that the data centres of UK businesses might have in the face of emergent energy supply risks. The focus for investigation was between 1990 and 2006, being the period in which worsening weather patterns and increasing threats to energy security have become pronounced. It is also the period of time that the Peak Oil theory and other concerns around hydrocarbon depletion have come to the fore. The study involved an examination of government policy with regard to UK energy security and strategy and an assessment of the business continuity approaches adopted by UK businesses. The research demonstrated that whilst most companies have made provision for local power disruptions, there is very little awareness of the increasing risks arising from the twin spectres of hydro-carbon depletion and global warming, combined with the exacerbating factors of poor infrastructure investment, market liberalization and deliberate acts. Communication from government on these risks is not widespread. The type of scenario that would likely occur as a consequence of these risks has been shown to be of longer duration and wider impact than the typically local incidents that have occurred over the last two decades. Consequently, it is suggested that variables such as speed of onset, forewarning and duration of event should

become more important in planning. Unfortunately, in the majority of cases, the approach to business continuity reflects a more traditional view of risk. The results also suggest that disaster recovery specialists may themselves not be aware of the risks, and therefore the trust placed in them by businesses seeking specialist knowledge is called into question.

6.3 Policy Recommendations

The key recommendation arising from the study, and one highlighted by a number of participants, is that the UK government must become more proactive in communicating emergent risks to the business community, although it is accepted that there is a balance to be found between communication and anxiety. As one participant put it "this government isn't good at communicating, so if it suddenly started doing it, well, it might just upset the applecart".

During the research, two respondents commented that they were surprised that their own business continuity advisors had not identified the emergent risks described. To address this issue, it is critical that the business has access to advisers, whether internal or external, who have a real awareness of upstream supply issues. As the research has shown, few, if any, of the advisors used by companies in the survey, had any real awareness of the issues around hydro-carbon depletion. If the company does not have adequate internal expertise, identifying an external advisor experienced in this field should be considered a priority.

The lack of effective risk assessment is highlighted as an area of concern. This was discussed at length with one interview participant with BCP responsibility and it was felt that the Key Intelligence Topics/Questions approach [Herring, 2001] would be an effective method for capturing the relevant information. A proposed framework under which this

exercise could be carried out, and suggested areas for investigation, are contained in Appendix C. The model will not only allow identification of risks, but it will assist in identification of early warnings, which will allow early intervention when events are signaled. Additionally, a suggested modification of the standard risk scoring to include measures for forewarning, duration of event and speed of onset as recommended by Wold and Shriver [1997] is proposed [Appendix C, Figure 3]

What shape any mitigating actions will take will depend to an extent on the resources available to the individual company. Many of the actions that can be taken to address the specific issues outlined in this paper are no different to typical business continuity activities. However, the issue is perhaps one of scaleability. If and when instability does become a regular feature of UK electricity supply, the measures that are taken will need to be constantly reevaluated to stay ahead of the situation. One individual commented that as investment in a data centre is planned 2-5 years in advance, there would need to be clear evidence that the risk was real before the design (and cost model) could be modified to address this.

As has been seen, the likely impact of an event considered in this study would be either geographically widespread, or of long duration, possibly including programmed brown-outs. The most obvious way of avoiding this would be to diversify the method of powering the business. However, as all businesses are dependent on electricity, this is not feasible. There are a number of options that could be considered to provide alternative methods of obtaining that electricity.

Within the UK, the majority of traded electricity is carried via the national grid; there is very little choice in terms of supplier – the pricing may be better, but the underlying transmission infrastructure – and thus susceptibility to outage - is the same. However, by

looking further afield this level of diversification might be possible. For example, the fact that Britain's ability to stockpile gas is significantly lower than that elsewhere in Europe [Walter, 2007] might mean that placing a secondary data centre in another European country would make sense. In the case of a very cold winter, where gas demand exceeds supply, the UK might well be forced to implement the measures described in the literature – and as has been seen in the literature, this situation was narrowly averted in the recent past , a fact that alone is suggestive of a real risk.

An alternative approach might be to site a secondary data centre in a country that has a lower dependence on gas or other hydro-carbons for electricity generation. A country such as Norway, with over 90% of electricity being produced from renewables, or France, with 78% being produced by nuclear power stations [WSS, 2006] might be a good choice. Companies for whom such an investment can be justified would be well advised to consider it. If this investment is too high, another option, which might protect against supply outages caused by freak weather, but would not protect against prolonged, country-wide outages caused by fuel shortages, is simply to build a secondary data centre in the UK, but in an area sufficiently distant from the main centre as to ensure that even extensive damage would not affect operations. A number of large London based companies have multiple data centres within the M25, often based in the premises of professional outsourcing providers. These centres are often some miles apart, but might not protect against a significant incident. Once again, such an investment warrants consideration and was certainly uppermost in the minds of all of those who were interviewed during the course of the project.

Finally, most of the companies (77%) in the sample had invested in backup generators. As a cost effective minimum solution, even smaller companies should consider this investment. However, such investment must be undertaken in the context of a holistic review of the

company's vulnerabilities, including interfaces with telecommunications providers and support contractors, if it is to bring benefits.

6.4 Limitations of Study

There is little existing literature that deals specifically with the impact of fossil-fuel depletion on business. Present research appears to be concentrated on macro-effects and does not appear to have begun to consider the impact on individual businesses.

The study was necessarily limited to consideration of data centre impacts. Clearly, energy shortages would have a very serious impact on the daily mobility of the workforce and on industry's ability to transport both raw materials and finished goods.

The increasing focus that is coming to bear on business continuity practices is largely positive for best practice; however, it has also made gaining access to information about a company's approach to business continuity much more difficult. This is because accidental disclosure could have a detrimental effect on share prices and reputation. Consequently, some of the recommendations made in the study were made based on experience within a very small sample of businesses.

6.5 Contributions to existing knowledge in the areas of Power and Energy Supply

The research has identified a number of vulnerabilities that businesses will have in the event of supply disruption and has proposed revisions to existing risk assessment models to take account of emergent risks. It has identified the additional level of risk that UK businesses are exposed to as a consequence of the infrastructure and geography of the nation and

clarified the role that the UK government is taking in addressing security of supply and the climate change agenda.

Furthermore, it is perceived that documented best practice, to which businesses turn when planning their business continuity strategy, may trail recent events in terms of the risks to energy supply. It is therefore hoped that this topic – and specifically the recommendations regarding risk assessment and cost benefit analysis - will bring benefits to businesses in the UK by enabling them to better plan for contingency events in their business continuity planning processes and through specific investments.

6.6 Areas of Further Research

As this is a broad study area, the specific scope of the study was limited to companies with computing data centres within the British Isles. Further research is urgently needed into the likely effects of sustained energy shortages on workforce mobility, logistics and transport of essential goods.

Research is also recommended into the relationship between government policy and best practice as it affects professional advisers in the field of continuity planning. Little evidence was found to suggest that such a relationship exists and, as such advisers are key to the dissemination of information to smaller businesses particularly, this is a key concern.

6.7 Conclusion

Chapter Six concludes the study and has presented the conclusions and key policy recommendations arising from the study. It has identified limitations in the research undertaken, and has presented recommendations for further research that will assist in further protecting UK businesses from energy supply events.

Bibliography

Alexander. (1997) *Middle East gas export bound to rise considerably*. Alexander's Gas & Oil Connections Reports. [Online] Available from: http://www.gasandoil.com/goc/reports/rex74609.htm Accessed on 19th July 2006.

AUA. (2007). *Nuclear Power in the United Kingdom*. Australian Uranium Association. [Online]. Available from: www.uic.com.au/nip84.htm Accessed on 20th April 2007

Awerbuch, S. (2003). *Determining the Real Cost – Why renewable power is more cost-competitive than previously believed.* Renewable Energy World March – April 2003. James & James Publishers. [Online] Available from : http://www.jxj.com/magsandj/rew/2003_02/real_cost.html Accessed on 6th July 2007

Bainerman, J. (2005). Peak Gas- Is there a looming shortage of Natural Gas. Resource World. February 2005. [Online] Available from: http://www.admiralbay.com/global/contentserver/files/1022/150190_resourceworld.pdf Accessed on 12th July 2007

BBC. (2006a). *Ukraine "stealing Europe's gas"*. BBC News. [Online] Available from http://news.bbc.co.uk/1/hi/world/europe/4574630.stm Accessed on 22nd July 2006.

BBC. (2006b). *Gas shortage sends prices soaring*. BBC News. [Online] Available from http://news.bbc.co.uk/1/hi/business/4802786.stm Accessed on 22nd July 2006.

BBC. (2007). *On this Day – 15th September*. BBC News. [Online]. Available from : http://news.bbc.co.uk/onthisday/hi/dates/stories/september/15/newsid_2518000/2518707.stm Accessed on 29th April 2007

BBC. (2007b). *Flooding causes chaos in country*. BBC News. [Online] Available from: http://news.bbc.co.uk/1/hi/england/south_yorkshire/6755459.stm Accessed on 29th June 2007.

BBC. (2007c). *Three dead following flood chaos*. BBC News. [Online] Available from: http://news.bbc.co.uk/1/hi/uk/6236348.stm Accessed on 29th June 2007.

BCI. (2004). *Business Continuity Research*. Business Continuity Institute. [Online] Available from : http://www.thebci.org/BCIResearchReport.pdf Accessed on 22nd July 2006

Benson, C. (2005). Measuring Mitigation – Methodologies for Assessing Natural Hazard Risks and the Net Benefits of Mitigation. Provention Consortium. [Online] Available from: http://www.unisdr.org/wcdr/thematic-sessions/presentations/session3-7/porvention-dr-benson.pdf Accessed on 27th July 2007.

Bjorkqvist, O. (1996). Perspectives on Demand Side Energy Efficiency. Sweden. [Online] Available from : http://bjorkqvist.nu/thesis/thesis.htm#Literature Accessed on 7th July 2007. para 15

BNG. (nk). *Operations Portfolio*. British Nuclear Group. [Online] Available from : http://www.britishnucleargroup.com/section.php?pageID=186 Accessed on 20th April 2007

Cheng, E. (2004) Energy Crisis Looms over China. Green Left Weekly. [Online] Available from : http://www.countercurrents.org/peakoil-cheng300504.htm Accessed on 20th July 2007.

City of Concord. 2001. *Economic Insight*. Fall 2001 Edition. [Online] Available from : http://en.wikipedia.org/wiki/Energy_use_and_conservation_in_the_United_Kingdom Accessed on 7th July 2006

D'Antoni. (2003). *Business Continuity Slides Down the Priority Scale*. Information Week. [Internet] Available from: http://fcweb.embanet.com/Login/FAV9-00066137/FAV9-0009D3E9/FAV9-0009D3EA/FAV9-000FDD92/FAV9-000EE1CB/FAV9-000EE1CA/ Accessed on 29th June 2007

Darley, J. (2004) *High Noon For Natural Gas – The New Energy Crisis*. US: Chelsea Green Publishing Company, pg 14-15.

Defra. (2005). Progress towards national and international targets. Department for Environment, Food and Rural Affairs. [Online] Available from: http://www.defra.gov.uk/environment/climatechange/uk/progress/index.htm Accessed on 6th July 2007

DTI. (N.K) *Information Security – Understanding Business Continuity Management.* Department for Trade and Industry. [Online] Available from: http://www.dti.gov.uk/files/file9952.pdf pg 8. Accessed on 22nd July 2006

DOI. (2005). *Daily Post Hurricane Gulf of Mexico Oil and Natural Gas Production Report*. Department of the Interior Minerals Management Service. [Online] Available from : http://www.doi.gov/katrina/ Accessed on 9th June 2007.

EQE. (N.K) *E.Q.E Summary Report – The European Storms Lothar and Martin*, Dec 26-28 1999. EQE. [Online] Available from http://www.absconsulting.com/resources/Catastrophe_Reports/Lothar-Martin%20Report.pdf Accessed on 3rd October 2006

Frost, C. (1994) *Effective Responses for Proactive Enterprises: Business Continuity Planning. Disaster Prevention and Management*. MCB UK Ltd. [Online] Available from: http://www.emeraldinsight.com/Insight/viewContentItem.do?contentType=Article&contentId=870828 Accessed on 22nd July 2006

Grubb, M. Butler, L. Sinden, G. nk. *Diversity and Security in UK Electricity Generation – The Influence of Low Carbon Initiatives*. Cambridge-MIT Institute. [Online]. Available from : http://www.eci.ox.ac.uk/research/energy/downloads/sinden-cambridge.pdf Accessed on 29th April 2007

Graydon, I. (2005). *Business Continuity for the SME. An Investigation into the strategic challenges affecting the planning and execution of business continuity plans within UK small and medium sized businesses*. UoL. [Online] Available from: http://fcweb.embanet.com/Login/FAV9-00066137/FAV9-0009D3E9/FAV9-0009D3EA/FAV9-000FDD92/FAV9-000EE1CB/FAV9-000EE1CA/ Accessed on: 29th June 2007 pp34

Hall, D. (2004) Experience with liberalization and privatization of electricity. University of Greenwich. [Online] Available from: http://www.psiru.org/reports/2004-04-E-indon.doc Accessed on 16th July 2007

Hales, S. (2003). Reaping the Rewards of Effective Business Continuity Management. KPMG. [Online] Available from: http://www.isaca-london.org/presentations/ISACA%20-%20MASTER%20VERSION%203%20%5BRead-Only%5D.pdf Accessed on 27th July 2007

Herring, J. (2001). *Key Intelligence Topics : A process to identify and define intelligence needs*. Competitive Intelligence Review. Volume 10 Issue 2 pp 4-5

Hodgson, P. (2004). *Gas Supplies to the UK – a review of the future*. Institute of Physics. [Online]. Available from: http://ioppublishing.com/Our_Activities/Science_Policy/Publications/file_4153.pdf Accessed on: 19th July 2006. Figure 1

House of Commons. (2004). *Resilience of the UK electricity network – Third Report of Session 2003-2004*. House of Commons Trade and Industry Committee. [Online] Available from: http://www.publications.parliament.uk/pa/cm200304/cmselect/cmtrdind/69/69.pdf Accessed on: 29th June 2007 pp7-8

House of Commons. (2004b). *Third Report of Session 2003-2004*. House of Commons Trade and Industry Committee. [Online] Available from: http://www.publications.parliament.uk/pa/cm200304/cmselect/cmtrdind/69/6902.htm Accessed on: 29th June 2007

Johansson, J. Lindahl, S. Samuelsson, O. Ottosson, H. (2006) *Synopsis: The Storm Gudrun – A Seven Weeks Power Outage in Sweden*. [Online] Available from: http://www.cris2006.com/downloads/Synopsis/cris2006_ND4.pdf#search=%22power%20outage%20sweden%20filetype%3Apdf%22 Accessed on 3rd October 2006

Lanz, J. (2002). *Business Continuity Planning- A Risk Manager's Agenda for Operational and Credit Risk Management*. IT Risk Management. [Online] Available from: http://www.itriskmgt.com/downloads/articles/March%202002%20-%20RMA%20-%20BCP.pdf Accessed on 27th July 2007.

Lovins, A. *Four Revolutions in Electric Efficiency*. Contemporary Policy Issues. Vol 8 No3. pp122 – 141 (cited in Bjorkqvist, 1993)

Mechler, R. (2005) *Cost benefit analysis for disaster risk management* (proceedings of Session 3 of World Conference on Disaster Reduction). WCDR. [Online] Available from: http://www.unisdr.org/wcdr/thematic-sessions/thematic-reports/report-session-3-7.pdf Accessed on 27th July 2007.

Mingay, S. (2006) *Business Continuity Questions from European Midsize Businesses*. Gartner Research. ID Number G00141799

Mitchell, J. (2000) *Energy Supply Security: Changes in Concepts*. Mitchell. [Online] Available from: http://www.chathamhouse.org.uk/pdf/research/sdp/EnergySupplySurityforPDF.d.pdf Accessed on: 22nd July 2006.

National Grid. (2007). *What is LNG ?*. National Grid. [Online] Available from : http://www.nationalgrid.com/uk/Gas/lngstorage/What/ Accessed on 6th July 2007.

Nickolett, C. (2006). An overview of the Disaster Recovery Planning Process – From Start to Finish. Comprehensive Consulting Solutions Inc. [Online] Available from : http://www.comp-soln.com/DRP_whitepaper.pdf Accessed on 28th July 2007.

Njemanze, H. 2007. *SCADA Security Protections are on the Increase*. Pipeline and Gas Journal. February 2007. [Online] Available from: http://www.arcsight.com/articles/ArcSight_SCADA_Security_Protections.pdf Accessed on 29th April 2007

OFGEM. (1999), *Priority Gas Customer Arrangements – Modification of the Public Gas Transporter Licence – A decision document*. OFGEM. [Online] Available from : http://www.ofgem.gov.uk/temp/ofgem/cache/cmsattach/1182_pcnov.pdf Accessed on 22nd July 2006

Odenwald, S. (2001). *The 23rd Cycle:Learning to live with a stormy star*. Columbia University Press. 2001. Chapter 1. Pg 1 -14.

Oil & Gas UK. (2004). *Gas – The UK's Fuel of Choice*. Oil & Gas UK. [Online]. Available from: http://www.oilandgas.org.uk/issues/gas/index.cfm. Accessed on 9th June 2007

Passmore, R. (2007) *Best Practices Yield High Availability Storage Area Networks*. Gartner Research. ID Number G00147059.

POST (Parliamentary Office of Science and Technology). (2001). *UK Electricity Networks. Postnote Number 163*. Parliamentary Office of Science and Technology. [Online] Available from: http://www.parliament.uk/documents/upload/post/pn163.pdf. Accessed on 19th July 2006.

POST (Parliamentary Office of Science and Technology). (2003). *The Nuclear Energy Option in the UK. Postnote Number 208*. Parliamentary Office of Science and Technology. [Online] Available from: http://www.parliament.uk/documents/upload/postpn208.pdf page 4 para 6. Accessed on 19th July 2006.

POST (Parliamentary Office of Science and Technology). (2004). *Terrorist Attacks on Nuclear Facilities. Postnote Number 222*. Parliamentary Office of Science and Technology. [Online] Available from: http://www.parliament.uk/documents/upload/postpn222.pdf. Accessed on 9th October 2006.

POST (Parliamentary Office of Science and Technology). (2003). *The Nuclear Energy Option in the UK. Postnote Number 208*. Parliamentary Office of Science and Technology. [Online] Available from: http://www.parliament.uk/documents/upload/postpn208.pdf page 3. Accessed on 19th July 2006.

Poulson, K. 2003. *Slammer Worm Crashed Ohio nuke plant net*. The Register. [Online] Available from: http://www.theregister.co.uk/2003/08/20/slammer_worm_crashed_ohio_nuke/ Accessed on 29th April 2007

Riptech. 2001. *Understanding SCADA System Vulnerabilities*.Riptech. [Online] Available from: http://www.iwar.org.uk/cip/resources/utilities/SCADAWhitepaperfinal1.pdf Accessed on 29th April 2007

Roberts, P. (2004b) *The End of Oil – the decline of the petroleum economy and the rise of a new energy order*. London: Bloomsbury Publishing, 45-65.

Robelius, F. (2007). *Giant Oil Fields – The Highway to Oil*. Uppsala University. [Online] Available from http://publications.uu.se/abstract.xsql?dbid=7625 Accessed on 15th July 2007.

Salomone, S. (2006). *Solar Flares Imperil Grid*. EnergyBiz Magazine. May/June 2006. Pg 88. [Online] Available from: http://energycentral.fileburst.com/EnergyBizOnline/2006-3-may-jun/Solar_Flares.pdf#search=%22solar%20flare%20cycle%20filetype%3Apdf%22 Accessed on 3rd October 2006.

Savage, M. (2002) *Business Continuity Planning*. Work Study. MCB UP Ltd. Volume 51. Issue 5. Pg 254 – 261 [Online] Available from: http://www.emeraldinsight.com/Insight/viewContentItem.do?contentType=Article&contentId=851392 Accessed on 22nd July 2006.

Shea, D. 2003a. *Critical Infrastructure: Control Systems and the Terrorist Threat*. Congressional Research Service. [Online] Available from: http://www.fas.org/irp/crs/RL31534.pdf Accessed on 29th April 2007. PP 9-11

Sinden, G. 2006. *Renewable Electricity Generation*. DTI. [Online] Available from: http://www.dti.gov.uk/files/file30091.pdf. Accessed on 5th June 2007.

Continuity Central. (2005). *Central London Data Centres – Too many eggs in one basket ?.* Continuity Central. [Online] Available from: http://www.continuitycentral.com/news02223.htm Accessed on 29th June 2007

Sungard. (2006). *Lessons Learned from Hurricane Katrina : How to maintain Operations during a regional disaster*. Sungard. [Online] Available from: http://www.availability.sungard.com/NR/rdonlyres/82F6AB24-C25C-448A-A988-5EAA94CE7AD0/0/LessonsLearnedfromKatrina.pdf Accessed on 6th June 2007

Thomas, S. (2004). *The British Model in Britain: Failing Slowly*. University of Greenwich. [Online] Available from: http://www.psiru.org/reportsindex.asp Accessed on 13th July 2007.

Thomas, S. Hall, D. (2003). *Blackouts: Do liberalization and privatization increase the risk ?* University of Greenwich. [Online] Available from: http://www.psiru.org/reportsindex.asp Accessed on 13th July 2007

Tregaskes, R. (2002). *Business Continuity Planning – What, When, Who, How*. ARUP Security Consulting. [Online] Available from: http://www.arup.com/_assets/_download/download247.pdf Accessed on 27th July 2007

Truitomo, S. (2005). *Cost benefit analysis for disaster risk management* (proceedings of Session 3 of World Conference on Disaster Reduction). WCDR. [Online] Available from: http://www.unisdr.org/wcdr/thematic-sessions/thematic-reports/report-session-3-7.pdf Accessed on 27th July 2007.

UCSD. (1999). *Voltage Cut to Improve Power Woes*. El Mercurio. [Online] Available from : http://ssdc.ucsd.edu/news/chip/h99/chip.19990224.html Accessed on 29th June 2007

Walter, J. 2007. Cash in on Gas Storage Shortage. Yahoo Finance. [Online] Available from : http://uk.biz.yahoo.com/14052007/35/cash-gas-storage-shortage.html Accessed on 6th July 2007.

Wikipedia, nk. *Energy use and conservation in the United Kingdom*. [Online] Available from : http://en.wikipedia.org/wiki/Energy_use_and_conservation_in_the_United_Kingdom Accessed on 7th July 2006

Winecki, L. (2004). *45% of companies willl (sic) have two data centres by 2008*. Global Continuity. [Online] Available from: http://www.globalcontinuity.com/thought_leadership/45_of_companies_willl_have_two_data_centres_by_2008 Accessed on 7th July 2007

Wold, G. Shriver, F. (1997) *Risk Analysis Techniques. Disaster Recovery Journal*. [Online] Available from: http://www.drj.com/new2dr/w3_030.htm Accessed on 12th July 2007

Woodman, P. 2007a. *Business Continuity Management*. Chartered Management Institute. [Online] Available from: http://www.ukresilience.info/upload/assets/www.ukresilience.info/bcm_report2007.pdf Accessed on 20th April 2007. pp 6 - 7

Woodman, P. 2007b. *Business Continuity Management*. Chartered Management Institute. [Online] Available from:

http://www.ukresilience.info/upload/assets/www.ukresilience.info/bcm_report2007.pdf

Accessed on 20th April 2007. pp 10

WSSG. 2006. *Wylfa Power Station Site Stakeholder Group – Response to the Government DTI 2006 Energy Review*. DTI. [Online] Available from:

http://www.dti.gov.uk/files/file31395.pdf Accessed on 5th June 2007

APPENDIX A – Survey Questionnaire.

This survey was promoted using the online tool SurveyMonkey.com. Additionally, 250 postal surveys were issued.

What is the primary fuel used for UK electricity generation ?

	Responses	*%*
Coal	15	41.7
Gas	6	16.7
Oil	10	27.8
Nuclear	4	11.1
Renewables	1	2.8
	36	

Does your business have an individual tasked with business continuity ?

	Responses	*%*
Yes	28	77.8
No	8	22.2
	36	

Are you familiar with the Peak Oil Theory ?

	Responses	*%*
Yes - very familiar	1	2.8
Yes - aware but not familiar	4	11.1
Yes	2	5.6
No	29	80.6
	36	

Where does the UK get most of its gas from ?

	Responses	*%*
North Sea/Domestic	23	63.9
Norway	4	11.1
Russia	7	19.4
Gulf States	1	2.8
Other	1	2.8
	36	

How long will the UK remain a net exporter of gas ?

	Responses	*%*

< 5 years	20	55.6
< 10 years	12	33.3
< 25 years	4	11.1
	36	

On balance, how do you rate the risk of a terrorist attack on the UK electricity supply in the next 5 years

	Responses	*%*
Very Low Risk	2	5.6
Low Risk	15	41.7
Medium Risk	12	33.3
High Risk	7	19.4
Very High Risk	0	0.0
	36	

There has been well publicised argument between Ukraine and Russia over gas supplies. In your view, what is the risk of such supply/market issues affecting UK electricity supply ?

	Responses	*%*
Very Low Risk	1	2.8
Low Risk	8	22.2
Medium Risk	15	41.7
High Risk	8	22.2
Very High Risk	4	11.1

In your view, does the weather pose a significant risk to electricity supply in the next 5 years ?

	Responses	*%*
Very Low Risk	2	5.6
Low Risk	14	38.9
Medium Risk	12	33.3
High Risk	7	19.4
Very High Risk	1	2.8

In your view, what is the risk of a supply issue arising from the design of the national grid for electricity and gas ?

	Responses	*%*
Very Low Risk	1	2.8
Low Risk	16	44.4
Medium Risk	14	38.9
High Risk	5	13.9
Very High Risk	0	0.0

In your view, does the weather pose a significant risk to electricity supply in the next 5 years ?

	Responses	*%*
Very Low Risk	2	5.6
Low Risk	14	38.9

Medium Risk	12	33.3
High Risk	7	19.4
Very High Risk	1	2.8

Does your organisation have a business continuity plan ?

	Responses	*%*
Yes	36	100.0
No	0	0.0

Just your business continuity plan just cover the operation of your computing/data centre or does it consider all aspects of the business ?

	Responses	*%*
Just the data centre	5	13.9
All aspects of the business	29	80.6
Don't Know	2	5.6

In the event of a failure, does your plan allow controlled shutdown of non-critical systems ?

	Responses	*%*
Yes	23	63.9
No	5	13.9
Don't Know	8	22.2

In the event of a failure, how much time can the company survive without non-critical systems ?

	Responses	*%*
Yes	23	63.9
No	5	13.9
Don't Know	8	22.2

If you are able to transfer services to another data centre, yours or a 3rd party's, how long will this take ?

	Responses	*%*
< 1 hour	9	25.0
1 hour - 8 hours	10	27.8
8 hours - 24 hours	6	16.7
24 hours - 48 hours	4	11.1
48 hours - 1 week	4	11.1
Other / No facility	3	8.3

If you are able to transfer services to another data centre, where is that data centre ?

	Responses	*%*
With UK	26	72.2
Other European Country	4	11.1
Asia	1	2.8
Americas	3	8.3
Other/No facility	2	5.6

Has your company ever considered locating a data centre in a

country such as Norway, where most electricity comes from renewables and there is less reliance on raw fuels ?

	Responses	*%*
Yes	1	2.8
No	27	75.0
Don't Know	8	22.2

If you answered yes to the above, what was the objective ?

	Responses	*%*
Cost Reduction	1	2.8
No answer given	*35*	*97.2*

How many separate power feeds does your data centre provide ?

	Responses	*%*
Only One	1	2.8
Two	17	47.2
More than Two	17	47.2
Don't Know	1	2.8

If you sought external advice, did the consultant discuss issues other than local design (eg upstream security, possible disruptions on a national level ?)

	Responses	*%*
Yes	8	22.2
No	5	13.9
Don't Know	19	52.8
No answer given	*4*	*11.1*

Do all your critical systems have power backup ?

	Responses	*%*
Yes	27	75.0
No	4	11.1
Don't Know	5	13.9

How long can your computing centre provide critical services during a power outage

	Responses	*%*
< 1 hour	3	8.3
1 hour - 24 hours	8	22.2
24 - 48 hours	4	11.1
48 hours - 1 week	2	5.6
> 1 week	13	36.1
Don't Know	5	13.9
Confidential	1	2.8

Do you use a diesel/petrol generator

	Responses	*%*
Yes	28	77.8
No	7	19.4

Don't Know	1	2.8

If you use a diesel generator, how many do you have at each site

	Responses	*%*
Just One	9	25.0
Two or more	19	52.8
Don't Know	1	2.8
Not applicable	7	19.4

If you use a diesel generator, how much fuel do you hold on site

	Responses	*%*
<24 hours	1	2.8
24 - 48 hours	5	13.9
48 hours - 1 week	4	11.1
1 week - 2 weeks	4	11.1
> 2 weeks	2	5.6
Don't Know	11	30.6
Not applicable	8	22.2
No answer given	*1*	*2.8*

Do you have a preferential agreement with a fuel supplier ?

	Responses	*%*
Yes	7	19.4
No	10	27.8
Don't Know	4	11.1
Not applicable	14	38.9
Confidential	1	2.8

If you do have a preferential agreement, how long will it take to replenish supplies ?

	Responses	*%*
< 24 hours	7	19.4
24 - 48 hours	1	2.8
48 hours - 1 week	2	5.6
don't know	14	38.9
Not applicable	9	25.0
Confidential	1	2.8
No answer given	2	5.6

How long can your telecommunications provider maintain services in the event of an outage ?

	Responses	*%*
< 24 hours	5	13.9
24 - 48 hours	3	8.3
48 hours - 1 week	2	5.6
1 week - 2 weeks	0	0.0
More than 2 weeks	4	11.1
Don't Know	21	58.3
Confidential	1	2.8

How often does your company test-run your generators, if you have them ?

	Responses	%
More than once per month	5	13.9
More than once per quarter	6	16.7
More than once per year	10	27.8
We don't	7	19.4
Don't Know	0	0.0
Not applicable	8	22.2

How often does your company perform full power failure tests ?

	Responses	%
More than once per quarter	3	8.3
More than once per year	13	36.1
More than once every two years	6	16.7
We don't	4	11.1
Don't Know	9	25.0
Not applicable	1	2.8

Does your company monitor actual power usage ?

	Responses	%
Yes	20	55.6
No	7	19.4
Don't Know	9	25.0

Do you forecast power requirements in advance ?

	Responses	%
Yes	19	52.8
No	16	44.4
Don't Know	1	2.8

How often does your company review its maximum power capacity available from suppliers ?

	Responses	%
Monthly	2	5.6
Quarterly	3	8.3
Yearly	7	19.4
No regular reviews	5	13.9
Don't know	19	52.8

Do you hold review meetings with power suppliers ?

	Responses	%
Monthly	0	0.0
Quarterly	4	11.1
Yearly	3	8.3
No regular reviews	12	33.3
Don't know	17	47.2

How often do you review the operational resilience of your data networks with your data supplier ?

	Responses	%
Monthly	5	13.9
Quarterly	7	19.4

Yearly	7	19.4
No regular reviews	7	19.4
Don't know	10	27.8

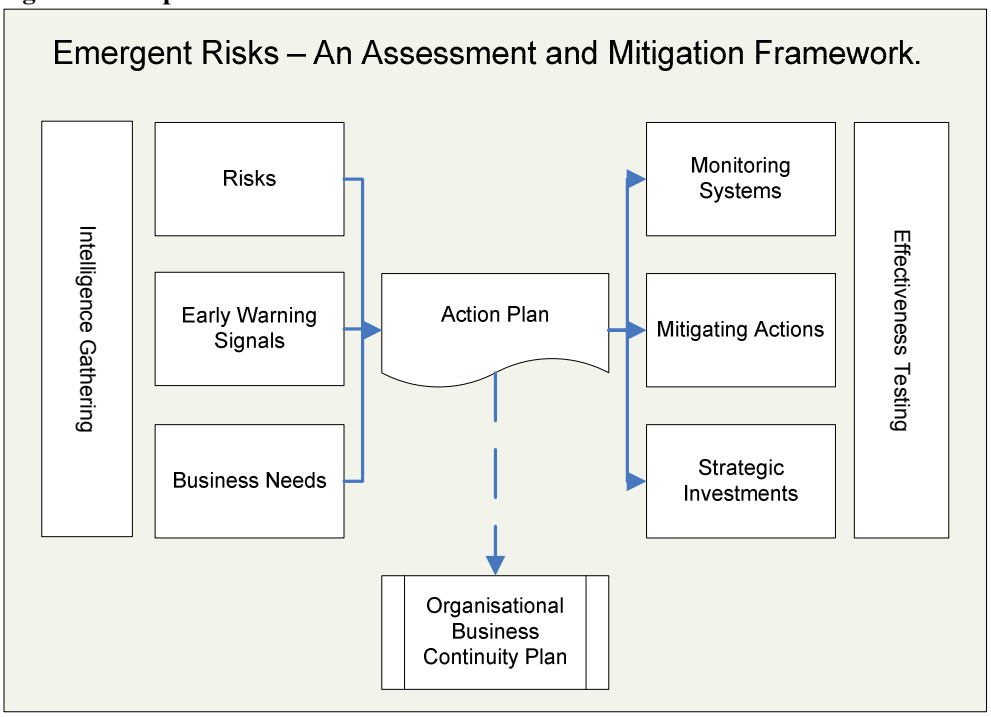
APPENDIX B – Schedule of Interview Questions

The following questions were addressed to the 5 interviewees who agreed to participate in the study.

1. What is your role with regard to business continuity ?
2. Where is business continuity positioned in the business (for example, is it an IT or a corporate function ?)
3. In your approach to business continuity planning, who did you consult for advice ?
4. How does your risk assessment process work and how comfortable are you that you are able to capture the risks and appropriate mitigating actions ?
5. You mentioned in your survey response that you were aware of the Peak Oil Theory. Is this a personal awareness or something that the company had actively investigated ?
6. You mentioned that you had talked to your power provider about resilience in their network. Did this cover simply local resilience or resilience at a national level ?
7. Do you feel that the government is doing an acceptable job in communicating emergent risks such as those arising from global warming or fuel depletion ?
8. Do you feel that you test your business continuity plans often enough ? In particular, if you have the ability to switch services between data centres, is the time estimate realistic ?
9. Do you think that micro-power generation might be a way to reduce your company's level of vulnerability to power outages ?
10. Based on your experience, what measures would you propose to a company without protection against power outage ?

APPENDIX C – Risk Assessment

Figure 1 – Proposed Risk Assessment Framework



Source: Young, J. (2007).
(Note: no previous graphical representation of a risk assessment model was found, the author lays claim only to the representation, not to the concept)

Figure 2 – Example Key Intelligence Topics/Questions

Key Topic	Key Question
Business Requirements	What service availability does the business require ?
	What systems must be available (critical systems) ?
	What wasthe impact on the business if access to these sytems is removed and how does this impact change over time ?
	How long can the business survive without key systems ?
	What is the cost of each day of downtime ?
	What backup processes can be put into place for each system (eg, paper based processes) ?
What risks could affect us ?	Are there any specific risks that arise due to our location (eg, flooding) ?
	Is our location likely to be impacted by war/acts of terror ?
	What does the electricity infrastructure look like in our region ? What deficiencies have been identified ?
	What raw fuel dependencies do we have in our region ?
	How will our government prioritise supplies in an emergency ?
	What is the likely impact of such an event on our environment ?

	What is the likely impact of such an event on our support staff ?
	How long will such an event last ?
	How long will it take to rectify damage arising from the event ?
	How long will such an event impact our staff ?
Early Warning Signals	How will early warnings be signalled for each type of event ?
	When will early warnings appear (length of forewarning)
	How will we ensure that we do not overlook minor signals that indicate a long term trend ?
	How will we monitor for these early warnings ? What media wasmonitored ?
	Who will monitor these early warnings ?
	Should we subscribe to external monitoring services ?
	Who will make decisions on actions to take based on these early warnings
	What evidence will we need to provide to brief this individual ?
	Does our external business continuity advisor (if appropriate) take the issues seriously enough ?
	Once a signal occurs, how long will it take for the full impact to be felt ?
Mitigatory Actions	What type of events does our existing business continuity plan cover ?
	What mitigatory action will we take for each event ?
	Which risks and actions are short term, and which are long term, in nature ?
	What is the cost of these mitigatory actions ?
	How will we document the processes to be followed when an event occurs ?
	How soon/late can mitigatory actions be initiated when an event occurs ?
	How will we test for shortfalls in planning ?
	Who wasresponsible for updating processes in line with changes in the environment ?
	How will we cope if key staff are unavailable to us during a crisis ?
	How will we cater for pastoral needs of staff during and after the crisis ?
	How will we accommodate staff who are unable to leave the site during the crisis ?
	How will we cope if public transport systems break down and staff are unable to travel to their office ?
	How will we cope if access to the data centre is denied to us ?
	Are there actions that we should take to improve resilience in our data centre ?

Source: Adapted from Herring (2001).

Figure 3 – Example Risk Register Entry

Item Number	(risk ID from Risk Register)
Risk Description	(description of risk)
Risk Rating	Measure of overall rating, calculated : (P * F * O * D) * I
Probability of Occurrence (P)	The likelihood of an occurrence. 1 = low, 5 = high
Forewarning (F)	The amount of warning of an event occurring 1 = significant warning, 5 = no warning
Speed of Onset (O)	The speed at which full impact wasfelt: 1 = slow, 5 = immediate
Duration of Event (D)	The duration of the event 1 = short, 5 = long
Impact (I)	The anticipated impact on the business: 1 = low, 5 = high
Mitigating Actions	What actions can be taken to mitigate the risk ?
Time to Implement Actions	The amount of time required to implement mitigatory actions, in days/months/years
Required Decision Point	The point at which a decision based on warning signs will need to be made if mitigatory actions are to be effective.
Early Warning Signals	What signals wasseen (eg, oil price rises, bad weather forecasts)
Frequency of Review	The frequency at which the current risk rating wasreviewed.
Risk Owner	Who in the organization is responsible for monitoring the risk
Date of Next Review	Date at which risk will next be reviewed

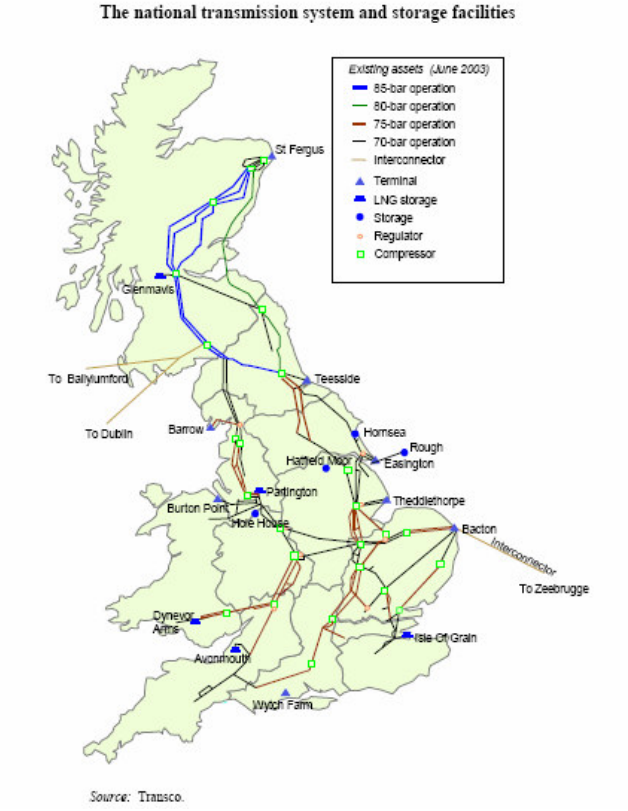
Source: Adapted from Herring (2001).

APPENDIX D – Selected Supportive Charts and Diagrams

Figure 4 - Electricity Flow Diagram 2001-2002

Source: POST (Parliamentary Office of Science and Technology). (2001). *UK Electricity Networks. Postnote Number 163*. Parliamentary Office of Science and Technology. [Online] Available from: http://www.parliament.uk/documents/upload/post/pn163.pdf. Accessed on 19th July 2006.

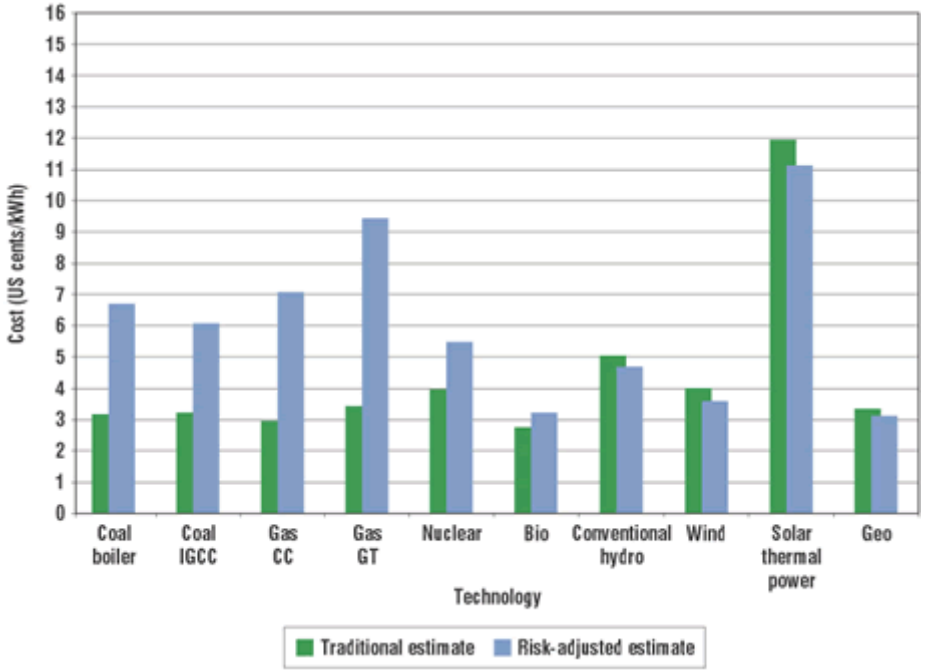
Figure 5 - National Transmission System and Storage Facilities



Source: National Grid. (2007). What is LNG ?. National Grid. [Online] Available from :

http://www.nationalgrid.com/uk/Gas/lngstorage/What/ Accessed on 6th July 2007.

Figure 6 - Risk Adjusted Cost of Electricity Estimates (Europe/IEA countries) based on historic fuel price risk



Source: Awerbuch, S. (2003). *Determining the Real Cost – Why renewable power is more cost-competitive than previously believed.* Renewable Energy World March – April 2003. James & James Publishers. [Online] Available from : http://www.jxj.com/magsandj/rew/2003_02/real_cost.html Accessed on 6th July 2007 pp 6