



Issues in Business Continuity Management

Rosemary Hill and Stephen Burgess
Victoria University
Melbourne, Australia

Graduate School of Business School of Information Systems
Kate.Hill@vu.edu.au Stephen.Burgess@vu.edu.au

ABSTRACT

The events of September 11, 2001 have markedly increased the level of awareness in organisations of business continuity management (BCM). Businesses can choose to adopt a risk management (reactive), or the more expansive crisis management approach (proactive) to BCM as they try to protect their business against the threat of a disaster. This paper discusses these two approaches to BCM, and then identifies a number of issues that businesses need to consider to provide them with the best possible chance of continuing their business in the event of a disaster. The areas of information technology, personnel management and senior management involvement are highlighted as being vital to the process of effective business continuity management. Examples of the importance of each of these areas to effective BCM are provided.

INTRODUCTION

The attack on the World Trade Center on September 11, 2001 challenged the way that many organizations thought about business continuity management (BCM) and the assumptions on which their business continuity plans were based. Companies had "spent millions on contingency plans, disaster recovery schemes and risk management techniques only to discover that in the face of a real catastrophe, they simply hadn't planned for the worst" (Rothfeder 2001). This paper examines some of the current approaches to BCM and identifies issues that the event raised in relation to business continuity management.

CONTRASTING APPROACHES TO BUSINESS CONTINUITY MANAGEMENT

The stark facts of September 11 are that the twin towers of the World Trade Center in New York collapsed as a result of a terrorist attack. The buildings housed nearly 1,200 businesses, which employed approximately 40,000 people (Ballman 2001a). Many people died and many other businesses in the vicinity were also affected.

In considering issues related to such a large-scale disaster, it is worthwhile looking first of all at the underlying approaches to business continuity management to see whether these may have any effect before examining the more detailed aspects of the process.

From the literature it is evident that there are two main approaches to business continuity management: the crisis management approach and the risk management approach.

The Crisis Management Approach

The crisis management approach positions business continuity management firmly in among all other organisational processes, such as strategic planning. It also implies the individuality of business continuity management. Organizations have different structures, different people and different histories so that if business continuity management is to be successfully developed and implemented within an organisation, it needs to take account of all these factors.

The crisis management approach is exemplified by Elliott, Swartz & Herbane (2002). This is based on the premise that:

- Business interruptions have both social and technical characteristics
- Organizations can create their own potential for failure
- Resilience can be built into an organisation through changes to processes and operating procedures
- A disaster can impact on a wide range of stakeholders both inside and outside the organisation.

An example that is frequently cited of the interaction of social and technical elements in a disaster is that of the Challenger disaster in 1986. This disaster resulted from a combination of a technical failure, that is, the faulty seals, and the organisational culture within NASA, which assumed that failure was impossible (Elliott, Swartz & Herbane 2002, p.3).

The Risk Management Approach

The alternative approach is that business continuity management exercise is a risk management exercise, which is based on the "five As" of risk management (Vancoppenolle 1999):

- Assess risk
- Accept or reject risk
- Avoid risk, transfer risk or reduce risk to acceptable level
- Analyse performance gaps
- Act to improve.

The aim is to hedge the risks of business interruptions, to develop a continuity strategy that meets the business objectives and to implement this strategy. This is an approach that has often been used by financial institutions.

The Approaches Compared

Risk management, in contrast with the crisis management approach, does not consider the concept of disasters or crises being caused by a combination of social and technical factors. Pauchant & Mitroff (1992 p. 183) state that the difference between the crisis management approach and the risk management approach is that "risk management involves evaluating the cost of a risk after multiplying by its probability of occurrence. A disaster with a high cost but a low probability of occurrence will not be taken into consideration. In contrast, crisis management involves focusing not only on the most probable events but also on the event with the greatest impact on its environment regardless of its probability of occurrence".

The other significant difference between the approaches is the attitude to people. In the risk management approach as described by O'Hehir (1999), operational risks include 'risks of human error or omission' such as unsafe behaviour and employee practices risks. Commercial risks include the loss of a key executive. There is no suggestion as there is in the crisis management approach that the culture and traditions of the organisation (which have developed as a result of the people within the organisation) have any impact on potential risks to the organisation.

The crisis management approach could be broadly described as a pro-active approach to business continuity management because it embraces the concept that some disasters can be avoided or mitigated if the organisation is willing or able to recognise the appropriate signals. The risk management approach is more of a reactive approach because it is based largely on assessing previous business interruptions and making judgements about the recurrence of these and assessing their impact on a particular business.

ISSUES RELATING TO THE BUSINESS CONTINUITY MANAGEMENT PROCESS

Whatever approach is used to BCM, the events of September 11 highlighted some problems with established business continuity plans, challenged some conceptions about what is important in the business continuity management process and raised some issues relating to the future of business continuity management.

Some of the more general problems that arose with established business continuity plans were (Global Continuity 2001):

- Many businesses had underestimated the total business effect of a disaster (Scannell, 2001; Berlind, 2001).
- Some plans failed because they were written on the assumption that any incident would only affect an individual building
- Plans that were too detailed were often less effective
- Many organisations need to be more realistic about what is actually possible in the aftermath of a disaster.

The more specific issues are discussed below. Whilst neither the risk management nor the crisis management approach could have provided a completely effective basis for dealing with the occurrences of September 11, it could be argued that a business which adopts a crisis management approach and which also addresses the following issues is well down the path to effective business continuity management.

Information Technology Issues

Many of the problems with established business continuity plans related to the recovery of information systems. This may be because business continuity management as a discipline has evolved from 'disaster recovery', the first phase of business continuity management in the 1970s when the aim of the continuity process was simply to recover data if the mainframe failed. In many organizations the IT recovery processes are still considered in isolation from the rest of the business processes. The focus of the IT recovery may therefore be on building sufficient redundancy into the system to replace any component that may fail regardless of whether each component is essential to get the business up and running again in the event of a disaster (Gondek 2002). It may, for example, be more cost effective to make plans to enable employees to work from home if necessary.

Similarly the provisions made for offsite facilities need to be carefully considered. Some organizations in the area of the World Trade Center had employed specialist disaster recovery services to provide offsite facilities in the event of a disaster. However, many of these disaster recovery services offered the same facilities to many companies (syndication) on the assumption that they would never all require the same facilities at the same time. The companies involved in any particular syndicate were not usually aware of the other partners in the group. Thus, on September 11th, many businesses found that the recovery venues were already occupied by others who were in the same disaster recovery syndicate. In one case, a firm called to invoke its provider some eight minutes after the event and was informed that they were the eleventh in line (Robinson 2002).

Some organizations also experienced problems with their back-up facilities. The Bank of New York, for example, had backup facilities, but found that they encountered problems when their back-up site had to deal with a customer's back up facility. These links could not cope with the volume of traffic, and they had not been fully tested and debugged (Hansell and Atlas 2001).

The scale of the disaster on September 11 also meant that many of the strategies for alternative communication methods were not work-

able because they had been based on the assumption that only one building might be affected in a disaster. Many websites were out of service for several days immediately after the attack as almost all fixed lines and mobile networks in the immediate area became inoperable. This was due to the destruction of critical supplier infrastructure, the saturation of the system by the volume of calls being made and the seizure of reserve bandwidth by the emergency services (Robinson 2002). This resulted in a virtual telecommunication blackout and this then had an immediate effect on any business based on the Internet. This too is an example of where previous disaster experiences had not been taken into consideration.

Personnel Issues

One of the most important issues to come out of the September 11 disaster is terms of business continuity management is the importance of people in the whole business continuity management process. On a purely practical level, many business continuity plans are based on the assumption that all employees will be available after a disaster and tasks to be carried out in the event of disaster are assigned on that assumption. The reality is that all employees may not survive and the business continuity plan must contain strategies to deal with that eventuality. The response of employees to a disaster may also be unpredictable. A person that has been assigned to a key role in the disaster recovery process may find that they cannot cope with the stress and cannot therefore carry out their assigned tasks (Global Continuity 2001; Honour 2001). In fact, stress and trauma for employees has not been considered in most plans (Sharp, 2001).

It is also important that employees are aware of their organization's continuity plans and have confidence that their organisation can deal with a disaster (DiNuzzo 2002).

In terms of resuming essential business processes after a disaster, employees must be considered as an essential part of these processes and their welfare must be considered. (DiNuzzo 2002).

The Importance of Senior Management Involvement

For many organizations, business continuity management is a new concept and is not part of their traditional methods for managing the business. For this reason, the first stage of the BCM process, the initiation stage, is necessary in order to 'sell' the idea of BCM to top management. This support from top management is essential in order to ensure that sufficient resources both human and financial are allocated to the BCM process and to ensure that the concept of BCM becomes embedded in the organisation (FSA 2002).

However, the maintenance of this commitment over a period of time and the ability or willingness of an organisation to learn from their own experience or from the experience of others is a concern for the future development of business continuity management.

In organizations which are not subject to regulation and/or legislation in relation to BCM there may be several reasons why it may be difficult to get support from top management. Psychological, cultural and economic factors all play an important role. Mitroff (2001 p.46-47) suggests various defence mechanisms that organizations use to deny their vulnerability to crises and which by inference persuade management that business continuity management is not a concern for them. These are:

- Denial – crises only happen to others
- Disavowal – crises happen, but their impact on us is small
- Idealization – crisis do not happen to good organizations
- Grandiosity – the organisation is so big and powerful it will be protected from crises
- Projection – if a crisis happens it must be because someone else is trying to harm us
- Intellectualization – the probabilities of a crisis are small and need to be measured precisely in terms of frequency of occurrence and expected outcomes
- Compartmentalization – a crisis cannot affect the whole organisation since each part of the organisation is independent.

Cultural differences also affect attitudes to disasters and this is increasingly significant with the globalisation of many companies. For example Nevola (1995) cites business tradition as a reason for the lack of contingency plans in Japan.

It is difficult to convince people to spend money to protect themselves against an event that may or may not happen. For this reason, spending on BCM is very often considered as discretionary expenditure, and when there is an economic downturn or budgets have to be cut for any reason, spending on BCM is often the first expenditure item that is cut (Myers 1999). Many organizations also consider that business, house and property insurance is sufficient although the contingent costs of disasters may equal or exceed the replacement costs (Jordan 1999).

One of the most potent factors for obtaining management support is previous experience of a disaster either in the same organisation or in a similar or neighbouring organisation (Pauchant & Mitroff 1992). However, there is evidence that interest in BCM is high immediately after a disaster and for a period afterwards, but that interest and commitment to it decline significantly. Handling of the 'Y2K' problem was an example of this and the decline of interest is also evident a year after the September 11 terrorist attacks. The Financial Services Authority (2002) reported that 'While there is no doubt awareness of BCM has increased since September 11, the level of awareness is still an issue in a number of firms'.

A SUCCESS STORY?

Merrill Lynch, one of the world's leading financial management and advisory companies, had its headquarters located directly opposite the World Trade Centre and about 9000 of its employees were affected by the terrorist attack. However, all its employees were evacuated safely and within a few minutes of the evacuation Merrill Lynch was able to switch its critical management functions to the command centre in New Jersey and continue in business (Ballman 2001b). The reason for this rapid resumption of business activity is directly attributable to the business continuity management practices in the company that reflect recognition of all the issues that have been discussed above. The Director of Global Contingency Planning at Merrill Lynch attributed their success to the fact that:

- They had the full support of top management and were willing to make the necessary investment in upgrading and testing the company's continuity plans
- They had taken advantage of the Y2K experience to upgrade and test their contingency plans
- All of their contingency plans had recently been overhauled
- All the contingency plans had been extensively tested
- The contingency plans had been disseminated throughout the corporation and all employees knew immediately where to dial into and transfer information
- The contingency plans were heavily focussed on the well being of the employees.

Maintenance of information systems, effective management of personnel and senior management involvement were vital to the 'success' of Merrill Lynch in this instance.

CONCLUSION

The events of September 11, 2001 increased the level of awareness in BCM. Whether businesses now adopt a risk management, or the more expansive crisis management approach to BCM, there are a number of issues they need to consider to provide them with the best possible chance of continuing their business in the event of a disaster. This paper has identified that issues related to information technology, personnel management and senior management involvement are vital to the process of effective business continuity management.

REFERENCES

- Ballman, Janette, 2001a, 'Terrorist attacks have far reaching effects on businesses', *Disaster Recovery Journal*, Fall 2001, [http://www.drj.com/special/wtc/1404-03.html] Accessed February 18, 2002.
- Ballman, Janette, 2001b, 'Merrill Lynch resumes business critical functions within minutes of attack', *Disaster Recovery Journal*, Summer 2001, [http://www.drj.com/special/wtc/1404-04.html] Accessed February 28, 2002.
- Berlind, David, 2001, 'Disaster planning goes IT', *CNET.com*, [http://www.zdnetindia.com/b...h/resources/ebusiness/stories/40395.html] October 11, 2001, Accessed November 1, 2001.
- DiNuzzo, John, 2002, 'The relationships factor in crisis management', *Contingency planning & management online*, [http://www.contingencyplanning.com/article_index.cfm?article=428] Accessed March 12, 2002.
- Elliott, Dominic, Swartz, Ethné and Herbane, Brahim, 2002, *Business Continuity Management*, Routledge, London and New York.
- Financial Services Authority, 2002, *A risk-focused review of business continuity management in major financial groups post September 11 2001*. [http://www.financialsectorcontinuity.gov.uk/home/pdf/fsa_bcm_paper_2002-09.pdf] Accessed December 16, 2002.
- Gondek, Richard, 2002, 'When more of the same isn't better', *Journal of Business Strategy*, Jul/Aug 2002, Vol.23, Issue 4, p.16.
- Hansell, Saul and Atlas, Riva D., 2001, 'Disruptions put Bank of New York to the Test', *The New York Times*, October 6, 2001 [http://www.nytimes.com/2001/10/06/business/06BONY.html?ei=1&en=3fcbfb41acd2ebe4&ex=1...10] Accessed October 8, 2001.
- Honour, David, 2001, 'Business continuity lessons learned from September 11th: A Summary', *Globalcontinuity.com*, [http://www.globalcontinuity.com], 12th December, 2001, Accessed December 14, 2001.
- Jordan, Ernest, 1999, 'IT contingency planning: management roles', *Information Management & Computer Security*, 7/5, pp.232-238.
- Mitroff, Ian I. with Anagnos, Gus, 2001, *Managing Crises Before They Happen*, AMACOM, New York
- Myers, Kenneth N., *Manager's Guide to Contingency Planning for Disasters*, Second Edition, John Wiley & Sons Inc., New York, 1999
- Nevola John, "The shock heard "Round the World", *Disaster Recovery Journal*, 1995, [http://www.drj.com/quake95.html] Accessed December 21, 1995.
- O'Hehir, Mike, 1999, 'What is a business continuity planning (BCP) strategy?' in 'Hiles, Andrew and Barnes, Peter (eds), *The Definitive Handbook of Business Continuity Management*, John Wiley & Sons Ltd, England.
- Pauchant, Thierry and Mitroff, Ian I., 1992, '*Transforming the crisis-prone organization*', Josse-Bass Publishers, San Francisco, U.S.
- Robinson, John R., 2002, 'Disaster recovery after September 11th', [http://www.jrcpl.com/Main/Article%20Disaster%20Recovery%20Feb02.htm] Accessed April 3, 2002.
- Rothfeder, Jeffrey, 2001, 'Brave new world', *CIO: Insight*, November 1, 2001, [http://www.cioinsight.com/article/0,3658,a=18364,00.asp] Accessed April 22, 2002.
- Scannell, Ed, 2001, 'Boss tells what he learned from Crisis', *Information Age*, October/November, p32-33.
- Sharp, John, 2001, 'September 11 2001', *Continuity*, Volume 5, Issue 4, Winter, p.2.
- Smith, Denis, 1990, 'Beyond contingency planning: towards a model of crisis management', *Industrial Crisis Quarterly*, 4, 263-275.
- Swartz, Ethné, Elliott, Dominic and Herbane, Brahim, 1995, 'Out of sight, out of mind: the limitations of traditional information systems planning', *Facilities*, Volume 13, Number 9/10, pp.15-21.
- Vancoppenolle, Geert, 1999, 'What are we planning for?' in Hiles, Andrew and Barnes, Peter (eds), *The Definitive Handbook of Business Continuity Management*, John Wiley & Sons Ltd, England.

Related Content

Hybrid Clustering using Elitist Teaching Learning-Based Optimization: An Improved Hybrid Approach of TLBO

D.P. Kanungo, Janmenjoy Nayak, Bighnaraj Naik and H.S. Behera (2016). *International Journal of Rough Sets and Data Analysis* (pp. 1-19).

www.irma-international.org/article/hybrid-clustering-using-elitist-teaching-learning-based-optimization/144703/

Particle Swarm Optimization from Theory to Applications

M.A. El-Shorbagy and Aboul Ella Hassanien (2018). *International Journal of Rough Sets and Data Analysis* (pp. 1-24).

www.irma-international.org/article/particle-swarm-optimization-from-theory-to-applications/197378/

Security of Identity-Based Encryption Algorithms

Kannan Balasubramanian and M. Rajakani (2018). *Encyclopedia of Information Science and Technology, Fourth Edition* (pp. 4975-4984).

www.irma-international.org/chapter/security-of-identity-based-encryption-algorithms/184200/

Adapting Big Data Ecosystem for Landscape of Real World Applications

Jyotsna Talreja Wassan (2018). *Encyclopedia of Information Science and Technology, Fourth Edition* (pp. 326-337).

www.irma-international.org/chapter/adapting-big-data-ecosystem-for-landscape-of-real-world-applications/183747/

An Efficient Server Minimization Algorithm for Internet Distributed Systems

Swati Mishra and Sanjaya Kumar Panda (2017). *International Journal of Rough Sets and Data Analysis* (pp. 17-30).

www.irma-international.org/article/an-efficient-server-minimization-algorithm-for-internet-distributed-systems/186856/