December 2002

Paradigm Shifts in Continuity Planning

Matthew Springer
University of Tasmania

Su Spencer
University of South Australia

Paradigm Shifts in Continuity Planning

Matthew Springer [a]

Su Spencer [b]

[a] School of Information Systems
University of Tasmania
Hobart, Australia
matthew.springer@utas.edu.au

[b] School of Accounting and Information Systems
University of South Australia
Adelaide, Australia

Abstract

This paper examines the continuity planning practices within two ISPs, and suggests the need for a paradigm shift in continuity planning for businesses in information industries, like Internet Service Providers. Instead of the standard risk management and disaster planning carried out by business, information industries need to focus on never failing to provide continuous service.

Keywords

Data Security EK01, Contingency Planning AF0401.04, Disaster Planning EK08, Service Quality EI0206.03, Small Business DA0201, Online IS GE01

INTRODUCTION

In a world where the way of doing business is becoming increasingly networked; in a world where businesses rely increasingly heavily on these networks; in a world where natural disasters, as well as man made disasters can lead to the failure of these networks, the provider of Internet services becomes a very important part of business. From the perspective of the Internet Service Provider (ISP), with enormous competition and cost pressures, the provision of continuous service can determine who retains customers and who loses to the competition.

In today's environment, it has become increasingly important to provide continuity of service to very demanding customers. There are many statistics being generated as to how damaging a break in service continuity can be for organisations: only 6% of businesses suffering from a catastrophic loss survive, 43% never reopen and 51% close within two years (Wilson, 2000). The IT popular media (Henderson, 2002) notes that where a 24-hour disaster recovery window used to be acceptable, it is quite unacceptable for a web-based supply chain or for Internet users such as Yahoo! and eBay.

Best practice solutions currently recommend identifying a manual alternative so that service can continue (ANAO, 2000; Wilson, 2000). This is workable within ordinary "bricks and mortar" organisations, and even within "bricks and clicks" organisations, but when it comes to the entirely information based business, with no bricks whatsoever; there may not be a manual alternative.

This notion of the necessity for a paradigm shift arose from a study into the continuity planning practices of two Tasmanian Internet Service Providers and an upstream provider of Internet service. The continuity planning study will be described below, followed by a discussion of the implications for new uses of Information and Communications Technology (ICT).

CONTINUITY PLANNING

The term "continuity planning" is a relatively new one, having been used for only around 10 years (Wheatman, 2001). It describes a process that has evolved from the Disaster Recovery Planning carried out for Data Centre Operations in the 1970s (King, 2000).

Continuity planning combines risk assessment (Paton, 1999), risk management (Pember, 1996; Cottell, 1997; Courtenay, 1997; Carlson and Parker, 1998; Higgins and Tilley, 1998; Iyer and Sarkis, 1998; Jordan and Musson, 1998; Bushell, 2000; Carson and Zawada, 2000; Rosenthal, 2000; Wieder, 2000; Wilson, 2000), disaster planning (Stair, 1983; Miller, 1984; Quarantelli, 1988; Haskett and Rohde, 1990; Lamond, 1990; Mahoney, 1993; Pember, 1996; Iyer, 1997), crisis management and business resumption planning (Rosenthal, 2000), into a package that seeks to stop problems occurring before they happen, and if they happen, get the business back to work as soon as possible (King, 2000). It is clear that the continuity planning approach is a much more holistic attitude to business than that of disaster recovery planning. A continuity plan is, "a set of processes developed for the entire enterprise, outlining the actions to be taken by the IT organization, executive staff, and the various business units in order to quickly resume operations in the event of a service interruption or outage" *(Wilson, 2000:25).*

Crisis management is what develops when there is a lack of continuity planning (Pember, 1996). Good continuity planning can avert the need for crisis management.

Business continuity views the organisation through the customers' eyes – what processes are most needed to meet the customers' expectations (King, 2000). It is necessary to take the problem planning process beyond simple disaster management and into the more holistic field of continuity planning. Disaster management is usually successfully carried out by the emergency services (Quarantelli, 1988). On the other hand, continuity planning is a way to, "address…low risk, high impact threats which cannot realistically be ignored without incurring the risk of massive and… long lasting cost penalties," (Lamond, 1990:38). An overall definition of continuity planning is: a holistic way to plan for the continuous operation of a business.

RESEARCH APPROACH

The research project was originally conducted as an Honours degree thesis by the first author, to investigate the nature of continuity planning within Tasmanian-based Internet Service Providers.

The data obtained came from interviewing subjects from within Tasmanian ISPs and a network provider. The research was approached as an intrepretivist study. Since the area of research is potentially sensitive, the researchers expected some resistance to the questioning, as well as possible subterfuge – or at least a cautious presentation of the "truth" – from the interviewees. Their views would be influenced by their levels of understanding, their desires to conceal information and their desires to help the researchers. Only through an interpretivist stance could the richness be taken from interview data and used for the benefit of the study.

This research project was intended to focus on a group of three Tasmanian-based ISPs. Although there are more than 30 ISPs operating in Tasmania (ABS, 2001) very few of them are Tasmanian companies and the three companies selected constituted the major part of the local ISP industry, being well established and operating throughout the state. Having such a small number of subjects was consistent with a qualitative study, focusing on depth of analysis, rather than generalisability (Miles and Huberman, 1994). Due to difficulties in gaining cooperation with certain Tasmanian ISPs, the project was then changed slightly to decrease the number of interviews required from ISPs and to include a network service provider.

In aiming to find out what level of continuity planning existed within Tasmanian ISPs, the obvious question of why this level existed came to the fore. Finding out why something happens is well suited to a qualitative research method, further supporting this research approach. Having decided that a qualitative method would be most appropriate for this research project, it becomes important to describe the research technique.

RESEARCH TECHNIQUE

Scope

This research was conducted with two ISPs that operate within Tasmania, and one upstream provider of network service to Tasmanian ISPs (a major telecommunications service provider). The researchers originally targeted the three dominant Tasmanian-based ISPs, but this proved impossible when one of the ISPs was continually "too busy" to be interviewed, and the researchers deemed that involving the upstream provider was a valuable extension to the study because of the supplier's relationships with the ISPs. The researchers were not interested in all of the ISPs' operations, or all of their planning practices, but only in their continuity planning practices.

The research question does lend itself to a much larger, quantitative study, where all the ISPs operating within Tasmania – or any other region in which businesses tend to have distinctive business styles and interactions with their customers and their suppliers – could have been surveyed. The researchers decided that it would be of more interest to find the reasoning behind continuity planning levels in a small number of ISPs with a common cultural base, than to survey the general, and unexplained, level throughout the more heterogenous industry sector.

Confidentiality

Continuity planning, by its very nature, can be very sensitive. Research into continuity planning can potentially highlight weaknesses within an organisation to those wishing it harm. It can also provide ammunition to customers in their fears about quality and continuity of service. In order to gain the most from the participants, enabling them to feel secure in the knowledge that what they said would be confidential, the firms have not been identified. The researchers provided formal written assurance of confidentiality to all participants, and interviews were conducted with the most senior people in the firms first, so that they could satisfy themselves of the appropriateness of the interviewer's approach.

Contact

Having identified three ISPs operating in Tasmania, the Managing Directors of each ISP was contacted via mail explaining the nature of the study and including a confidentiality agreement. After this initial contact, a phone call was placed to each Managing Director. The request was to interview three people within each organisation, preferably in different roles within the organisations. Each interview was to last for 45 minutes.

Although these ISPs were the dominant ones in Tasmania, they were still small businesses. Due to resource limitations within these small ISPs, the researchers had varying levels of success gaining participation from the ISPs. Although the small size of the organisations meant that it was possible to directly speak to two of the managing directors immediately, only one of them felt able to cooperate. Investing 135 minutes in a research study was considered unproductive time and too expensive for such a small business.

The third managing director was too concerned about confidentiality issues to agree to having any of his employees be interviewed, however he was willing to be interviewed. Through a fellow researcher, contact was made with a member of an upstream provider operating in Tasmania. The upstream provider's views have provided certain insights into the issues faced by ISPs from the supplier's viewpoint. At the end of the process, interviews had been carried out with the Managing Director, Technical Manager and Customer Service Manager of one ISP, the Managing Director of another, and a senior representative of the upstream network service provider.

Interview Process

The interview process consisted of a pilot interview and five other interviews that were included in the actual study.

Semi-structured interviews were used to obtain views from all of these participants. A set of subject areas was prepared before the interview, and the interviewer gently steered the interview in directions to cover these areas (Berg, 1998). During the interview, if a topic of

interest arose, the interviewer could follow this lead and then return to original topic areas. As an interview technique, this provided enough structure to gain the required information from the interviewees, without damaging the chances of achieving richness from the interview.

Questions examined the participants' experience and role within their organisations, as well as their experience with failures in service continuity. These were augmented by questions seeking to determine how closely aligned the practices of the organisations were compared to continuity planning best practice. The participants were also questioned about their role, or their staff's role in any continuity planning activities undertaken by the organisations, and what management's expectations of the staff would be. Questions were also asked regarding strategic planning within the organisations. This was thought to be potentially useful for determining the general approach that these organisations had to planning, or whether it was just continuity planning that was undertaken (or not undertaken).

DATA ANALYSIS

The interviews were recorded and transcribed. Having transcribed these interviews, it was possible to carry out data analysis on the written records of the interviews. In carrying out a qualitative study, enormous amounts of data are gathered through observations and interviews – so much information that it can become hard to handle. A way to deal with this influx of data is the use of a conceptual framework (Miles and Huberman, 1994). The conceptual framework used for this research was the bottom-up coding approach (Strauss, 1987; Miles and Huberman, 1994; Strauss and Corbin, 1998; Neuman, 2000).

The bottom-up coding approach involves taking the interview transcript and carrying out open, axial and selective coding. "Coding is analysis" (Miles and Huberman, 1994: 56). It is the analytic process through which data are fractured, conceptualised, and integrated to form theory (Strauss and Corbin, 1998). The bottom-up coding process represents a rigorous and verifiable method of analysing qualitative data (Miles and Huberman, 1994).

The coding process is designed to:

- Build rather than test theory.
- Provide researchers with analytic tools for handling masses of raw data.
- Help analysts to consider alternative meanings of phenomena.
- Be systematic and creative simultaneously.
- Identify, develop, and relate the concepts that are the building blocks of theory. (Strauss, 1987)

"Codes are tags or labels for assigning units of meaning to the descriptive or inferential information compiled during a study," (Miles and Huberman, 1994: 56). It is not the words themselves that matter, but the underlying meanings of the words (Miles and Huberman, 1994).

FINDINGS

Consistent with the amount of planning that small businesses tend to carry out, these small ISPs did not place a large focus on continuity planning either. One Managing Director stated that:

> *My personal attitude is that it doesn't get done at all costs, but it is so much a part of the way that we do business that it's always there and we just do it, but at the same time we have to assess whether it's cost effective or not. And what are the risks of something happening that we can't fix and if that risk is very, very low, we don't necessarily put anything in place.*

The ISPs were more likely to spend their resources on implementing system redundancy and uninterrupted power supplies so that the service would be continuous, rather than simply planning for it. A Managing Director stated:

> *It's [continuity planning's] been missed out in the past because we haven't had the staff capable of doing it.*

Another described the system redundancy that was being implemented:

> *Probably two options for the last mile, one is we use microwave from one supplier and fibre off the other suppliers.*

Similarly, a manager said in regard to system redundancy:

> *There are obvious things like hard disk crashes. We've had a lot of experience with those things happening. It's difficult to predict a hard disk crash and expensive to account for and we could use RAID systems. We don't use RAID, because it's relatively expensive. It's cheaper to just have a second server running than to have a RAID server.*

The findings suggested that the ISPs studied either did not carry out continuity planning at all, or carried out continuity planning if there were resources to do so, but mainly focused upon providing continuous service through technical solutions.

The culture within both ISPs was undoubtedly one of providing the best possible service to their customers. The way the two organisations went about this was considerably different, but both aimed to provide continuity of service to their customers. As far as planning cultures within the organisations, neither could truly be described as having a planning culture, but the differences here were also of note.

The two organisation's attitudes to customers could be explained through descriptions of times when the services failed. For one ISP, the problem was a major power failure, which resulted in the system going down for several hours. Most of the ISP's phones ran on electricity, and they were out also, however,

> *Standard phone power was up and running, so we had one analogue phone at the time. So we had to sit on one analogue phone and answer every call that came in, and say the service would be out until the power is restored.*

Comparing this to attitude of the other ISP where,

> *Providing a recorded response is more realistic.*

If there was a problem at the first ISP,

> *Generally speaking if it's a technical problem, there's not much we can do. It's a one-person fix. If a router's gone down, it takes one person to fix it – that's our technical manager.*

At the second ISP, with a more technically focused staff, all the staff would pitch in to solve the problem and get the service back up.

Both attitudes revolved around returning the service to normal as soon as possible, but one presented a personal face for the customers, the other a recorded one.

On the subject of their planning cultures, the ISPs were also quite different. As stated previously, the first Managing Director's view was that planning does not get done at all costs. Planning had been carried out within the firm when it was first established, even if it had not been recently revised. His view considered that,

> *It's really all been done, the planning's been done as far as we're concerned now. We haven't had to worry about it for a long time.*

The other Managing Director's view on formal planning was:

> *If you write these things down, things will be missed.*

In order to avoid missing things out of a formal plan, he chose to leave everything out of his plan. In effect this Managing Director's view was that planning was a very good practice, but writing plans down was the weak point of planning.

Although the ISPs interviewed within this research had vastly different attitudes to customers and business planning, their attitudes to continuity of service were the same: by investing in new technology for redundant systems, continuity of service could be provided.

DISCUSSION

In examining the opinions of those interviewed within the ISP, it was clear that although a formal type of continuity planning was not being carried out, both ISPs were actively working to implement system redundancy and system backups so that eventually they would reach a point where it would be very difficult for the service to be brought down.

Traditionally, organisations have been able to plan for business continuity by implementing safeguards for if normal business operations become impossible. Rather than spending resources on a formal planning process, the ISPs tended to use their available funds to provide backup servers, uninterrupted power supplies, multiple links to upstream service providers and alternative routing paths around the state of Tasmania.

Best-practice in the field of continuity planning would require that, as part of the risk assessment process methods of doing work manually should be considered (ANAO, 2000; Wilson, 2000). In a "bricks-and-mortar" business, the ability to accept cash over the counter and provide a written receipt would be perfectly satisfactory, allowing the exchange – money for goods or services – between the customer and firm. ISPs do not operate in such a way due to the nature of the business. ISPs are a pure information-selling service, based upon technology. ISPs are right there in the new information economy. An ISP can accept cash, and provide a receipt, but without the ability to enter this information into the computer system, there will be no way that access to the Internet can be granted. Further, if the Internet server is down, or the routing equipment has failed, there will be no service for the ISP to provide. Technology is required to supply access to the information in the information economy, and there is no manual substitute for the technology.

In the bricks-and-mortar world, a manual receipt book is a perfectly sensible continuity solution in case of a computer system failure. The idea of implementing technical solutions might be practical for a very large firm, but would be thoroughly unnecessary, expensive and ill advised for a smaller firm. On the other hand, a firm that is operating with services based upon information provision through a technological means has only technical solutions available to it, and so firms like the ISPs studied need to implement expensive technical continuity solutions as there are no manual equivalents to Internet access.

Elliott *et al*. (1999) have argued that Business Continuity Planning is a more strategic approach than technically focused Disaster Recovery, and that "better practice" organisations take a more holistic business view. While we agree that this is good management practice, it should not mask the fact that there are now many businesses that *are* their technology. No matter what the cause of system downtime, terrorist attack or straightforward hardware failure, the business must have replacement technology to stay in business. ISPs have been identified (ABS, 2001) as one of a new group of Information, Communication and Technology (ICT) industries that have arisen in recent years, and a critical service provider for businesses, householders and government. The differences between the bricks-and-mortar firms and knowledge-based firms that are representative of the Information Economy indicate a requirement for the development of a new continuity paradigm. The current best-practice literature recommends identification of systems that can be carried out manually so that in the face of system failure, the firm is not crippled (Pember, 1996). A new model needs to be developed for firms carrying out best practice continuity planning in the Information Economy to satisfy the need for firms that have no manual alternatives. Such a model would be extremely useful for application to firms such as Internet Service Providers, but certainly not limited to such.

It is ironic that while Information Systems leaders and educators are endeavouring to improve communication between business management and IT management, and to persuade general managers to take over planning functions from the technologists, new types of business drive some of the focus back onto the technical viewpoint. This will require a new balance to be negotiated, with the technical solutions paramount but still tackled in the context of strategic business requirements.

Firms like Amazon.com or Greengrocer.com are very much in the same situation as an ISP, and The Australian's feature writer identified Yahoo! and eBay (Henderson, 2002), and by inference suppliers of web services in the future. If the technology fails, there is no manual equivalent. Or, stretching the idea further, if banks continue in their path towards having no branches and only ATMs, if the technology fails in that situation then people could have no access to cash at all. Or slightly further into the future, where biometric testing might be required due to increased security levels at airports, what happens if that technology fails? Does it become a target for terrorist activity so that manual systems can be foiled, or is technology made so redundant and infallible that terrorist action cannot succeed?

In an information economy, where there are no manual alternatives given a break in continuity, new ways of planning for continuity need to be developed. It is this requirement for a paradigm change in continuity planning that this paper seeks to highlight. Our exploratory study showed that a prevention and redundancy approach is a natural enough progression for technical managers of technology-reliant businesses. However, they have not taken those steps in the conscious knowledge that they are operating in a different environment. Nor has the significance of technical prevention yet been acknowledged in the general management literature, which would seek a new balance between technical and non-technical continuity planning. It is hoped that further research will be carried out in this area.

CONCLUSION

In the information economy, the realms of continuity planning are being challenged. This is apparent in an information-based firm such as an ISP. The manual alternatives that underpin current continuity planning practices are of little or no value to information businesses. It is clear from the evidence presented that a paradigm shift needs to occur in the way that continuity planning is carried out for these firms. This shift needs to be considered and adopted to help ensure businesses' survival, and this is a particularly relevant philosophy in these uncertain times.

REFERENCES

ABS, 2001. Communications and Information Technology. Australian Bureau of Statistics. http://www.abs.gov.au/ausstats/abs@.nsf/0/518F2A16A89DEFDFCA256AB800808703?Open.

ANAO. 2000. *Business Continuity Management*: *Keeping the Wheels in Motion*. Australian National Audit Office. Canberra.

Berg, B. 1998. *Qualitative Research Methods for the Social Sciences*. Boston: Allyn and Bacon.

Bushell, S. 2000. Ready or Not? *CIO.*: 104-106, 108-109.

Carlson, S. J. and Parker, D. J. 1998. Disaster Recovery Planning and Accounting Information Systems. *Review of Business.* 19(2): 10-16.

Carson, D. and Zawada, B. 2000. Business Continuity Planning and the Ten Business Continuity Planning Pitfalls to Avoid in the "New Economy". *Disaster Recovery Journal.* 13(2): 74-77.

Cottell, R. 1997. Risk Management Awareness in Business Continuity Planning. *Survive.*: 14-15.

Courtenay, N. 1997. The Aim's the Same: Why Business Continuity Planning Should be a Risk Management Priority. *Survive.*: 21-22.

Elliott, D., Swartz, E. and Herbane, B. 1999 Just Waiting for the Next Big Bang; business continuity planning in the UK finance sector *Journal of Applied Management Studies* 8(1) 43-60

Haskett, J. and Rohde, R. 1990. Disaster Recovery Planning for Academic Computing Centers. *Communications of the ACM.* 33(6): 652-658.

Henderson, L. 2002 Disaster Recovery at Speed The Australian Technology Survey Series May 28,2002

Higgins, Y. and Tilley, K. 1998. Survey Highlights Need for More IT Security. *Business Insurance.* 32(24): 33.

Iyer, R. K. 1997. Enhancing Senior Management Awareness and Gaining its Jacobs, J. and Weiner, S. 1997. The CPA's Role in Disaster Recovery Planning. *The CPA Journal.* 67(11): 20.

Iyer, R. K. and Sarkis, J. 1998. Disaster Recovery Planning in an Automated Manufacturing Environment. *IEEE Transactions on Engineering Management.* 45(2): 163-176.

Jordan, E. and Musson, D. 1998. *Strategic Systems? Only When They Work!* ACIS.

King, J. 2000. Business Continuity Planning and the Highly Protected Risk Expanding the Envelope: Planning for the Entire Organization. *Disaster Recovery Journal.* 13(1): 28-30.

Lamond, B. J. 1990. An Auditing Approach to Disaster Recovery. *Internal Auditor.* 47(5): 38-49.

Mahoney, P. F. 1993. It's an Emergency - Do You Have a Plan? *Management Review.* 82(1): 45-49.

Miles, B. and Huberman, M. 1994. *Qualitative Data Analysis*. California: Sage.

Miller, M. 1984. Up From the Ashes...How Disaster Planning Can Keep You in Business. *Management Review.* 73: 44-50.

Neuman, W.L. 2000. Social Research Methods. Massachusetts: Allyn and Bacon.

Paton, D. 1999. Disaster Business Continuity: Promoting Staff Capability. *Disaster Prevention and Management.* 8(2): 127-133.

Pember, M. E. 1996. Information Disaster Planning: An Integral Component of Corporate Risk Management. *Records Management Quarterly*. 30(2): 31-37.

Quarantelli, E. L. 1988. Disaster Crisis Management: A Summary of Research Findings. *Journal of Management Studies.* 25(4): 373-386.

Rosenthal, P. 2000. *Business Resumption Planning*: *Justification, Implementation and Testing*. The Business Forum. http://www.bizforum.org/whitepapers/calstatela.htm. Accessed: 23 April 2001.

Stair, R. M. 1983. Computer Disaster Planning for the Small Business. *Journal of Small Business Management.* 21: 13-19.

Strauss, A. L. 1987. *Qualitative Analysis for Social Scientists*. New York: Cambridge Press.

Strauss, A. L. and Corbin, J. 1998. *Basics of Qualitative Research*: *Techniques and Procedures for Developing Grounded Theory*. California: Sage.

Wheatman, V. 2001. Aftermath: Disaster Recovery. *Gartner Research.*

Wieder, T. 2000. Risk Management. *Computerworld.*: 64.

Wilson, B. 2000. Business Continuity Planning: A Necessity in New E-Commerce Era. *Disaster Recovery Journal.* 13(4): 24-26.

COPYRIGHT