MACQUARIE GRADUATE SCHOOL OF MANAGEMENT

MGSM WORKING PAPERS IN MANAGEMENT

IT Service Continuity Assessment

Ernest Jordan

Macquarie Graduate School of Management

MGSM WP 2005-7

March 2005

Disclaimer

Working Papers are produced as a means of disseminating work in progress to the scholarly community, in Australia and aboard. They can not be considered as the end products of research, but a step towards publication in scholarly outlets.

© Ernest Jordan

Research Office

Macquarie Graduate School of Management
Macquarie University
Sydney NSW 2109
Australia

Tel +612 9850 9016
Fax +612 9859 9942

Email research@mgsm.edu.au
URL http://www.mgsm.edu.au/research

Director of Research A/Professor John Rodwell
Manager, Research Office Ms Kelly Callaghan

ISSN 1445-3029 Printed copy
1445-3037 Online copy

MGSM WP 2005-7

IT Service Continuity Assessment

Correspondence to:

Professor Jordan
Professor of Management
Graduate School of Management
Macquarie University, Ryde, NSW 2109
Australia

Telephone: + 61 2 9850 9041
Facsimile: + 61 2 9850 9019
Email: ernest.jordan@mgsm.edu.au
MGSM Site: http://www.mgsm.edu.au/

Abstract

IT service continuity is an area of IT-related risk that is assuming higher profile with the current concerns with corporate governance and IT governance. We present a model for IT service continuity that is compatible with IT governance thinking. The IT service continuity model uses performance measures in assessing the context, planning and outcomes of continuity management. The results of a survey of continuity preparedness in Australian government bodies are then described and used to test the model. Improvements to research instruments are suggested.

Keywords

Business continuity, IT continuity, IT governance

INTRODUCTION

Information technology is, for many organisations, the principle focus of their continuity planning – that is, their planning to restore normal business operations after some disruption. For some organisations, the idea of a break in IT services is unacceptable – systems may be regarded as 'mission critical' and set up to be 'fault tolerant'. For these organisations, duplicate facilities are the norm and a seamless switchover is an expectation. However, many surveys have shown that the majority of organisations do not take continuity seriously.

Over the last ten years issues of corporate governance have become widely known and have had such an impact that regulators have imposed new requirements for organisations. This renewed concern for corporate governance has been a significant factor in developing the demands for IT governance. This paper first reviews relevant aspects of the corporate governance literature and uses this to develop requirements for IT governance. The IT risks that an organisation faces need to be addressed by their IT governance practices and to this end an IT risk portfolio is described. This portfolio includes the risks that organisations face when IT services cannot be delivered.

Management responses to IT services continuity risks are commonly labelled 'disaster avoidance' and 'disaster recovery'. Management prepare 'business continuity plans' or 'disaster recovery plans' as a consequence of assessments of the business impacts of various outages. There is a substantial body of professional practice and endorsed 'good practice' in this area, however little research has been undertaken to determine whether organisations are investing sufficiently or getting sufficient rewards for their investments.

A previous model (Jordan, 2003) is enhanced to relate the organisation's IT service continuity risk context, to its IT service continuity planning activity and hence to the performance outcomes. Significant among these outcomes are the IT services' resilience to disruption and the ability to be able to recover IT services after going down. However to these benefits must be added the necessity of meeting requirements for regulators.

Corporate governance concerns with IT

While many would regard the concern of corporate governance with IT as relatively recent, it was raised as long ago as 1996, when Lindup pointed out that "information security" was of direct concern to board members (Lindup, 1996). He reported that the UK's Securities and Futures Authority (SFA) had warned its audience in the financial services industry that appropriate safeguards were to be taken for information, computer systems and networks, and that ultimate responsibility lay with directors. The term "information security" has been highlighted as this term is the subject of standards such as BS7799 (BSI, 1999) and ISO 17799 (ISO, 2002). However this term has a wide span, as specified in the standards, and deals with both continuity of services as well as the protection of assets. That is, there are both static and dynamic aspects. The stated goals are in dealing with the confidentiality, integrity and availability (CIA) of information.

Other researchers and authorities have continued to draw the link between corporate governance and information security (Holzinger, 2000; Williams, 2001; von Solms, 2001a, 2001b; Garigue and Stefanin, 2003; Bies, 2003; Herbane, Elliott and Swartz, 2004; Posthumus and von Solms, 2004). Herbane et al. (2004) in analysing case studies from financial institutions present a convincing argument for the strategic benefit that can accrue an organisation through the process of planning for business continuity, an argument that we take up later.

Professional practice has also moved along, with organisations now being able to be certified that they comply with BS7799. This certification is becoming more widespread with, for example, the Hong Kong Government mandating BS7799 certification for its service providers. Practitioners themselves can gain accreditation as advisers and certifiers. The Information Systems Audit and Control Association (ISACA, isaca.org) and Information Technology Infrastructure Library (ITIL, itil.org) also include continuity and security within their approaches.

IT governance

It is unrealistic to expect company directors to have direct and personal involvement with information security issues, and an intermediate process of IT governance is now being widely articulated. ISACA was among the first to identify the need to establish IT governance processes so that, in particular, an organisation's Audit Committee

would be able to make authoritative assessments on IT for the board's consumption. This is articulated in their COBIT methodology (ISACA, 2003) that has a strong audit stance. Jordan and Silcock (2005) on the other hand propose an IT governance approach that is proactive, enabling future IT projects to come within its ambit. This approach to IT governance is similar to that articulated as 'capability' by Peppard and Ward (2004).

The Jordan and Silcock (2005) model for IT governance adopts Markus's (2000) argument that all IT risks, not just those concerned with security or continuity, need to be brought together in an integrated approach. IT risks are assembled into a 'risk portfolio' that must be monitored through processes with which the board is confident (Jordan and Silcock, 2005). It further proposes that the complementary dimensions of IT governance that ensure its completeness are those concerned with IT benefits and IT strategy. It argues that if the board can be satisfied that IT risks, IT benefits and IT strategy are all being dealt with properly, the organisation's IT governance is in order.

The components of the risk portfolio, areas where IT can potentially give rise to negative business impacts, are given to be:

- Projects – failing to deliver;
- IT service continuity – business operations are reduced or stop;
- Information assets – are not protected and preserved;
- Service providers and vendors – do not deliver;
- Applications – systems fail the business;
- Infrastructure – foundations are inadequate; and
- Strategic and emergent – IT impacts on strategy. (Jordan and Silcock, 2005, p.49)

One advantage of this approach is that the static and dynamic aspects of 'information security' are separated. Information asset risks are concerned with the safeguarding of information, while the IT service continuity risk is concerned with only the continuous operation of IT systems that support the business. We continue with a discussion of IT service continuity and then develop a performance model that can be used by an organisation.

IT SERVICE CONTINUITY

Examples of IT service continuity failure are common across the business landscape but are generally rare for individual organisations. We illustrate the situation with two examples, the first being a denial of service (DoS) attack, driven by 'hacktivism'[1]:

> *"In February 2004 the SCO Group was the target of a denial of service attack linked to Mydoom, one of the fastest spreading email worms in history. The SCO website was rendered inaccessible and the site taken down. The company changed its domain name and moved to a new IP address." (AFR, 2004)*

The second example is much more mundane, the simple failure of the technology:

> *"Trading on the London Stock Exchange was disrupted for nearly eight hours by computer problems on Wednesday on what should have been one its busiest days of the year…*
> *The tax year expired on Wednesday and it is usually one of the exchange's heaviest days as thousands of retail investors buy and sell shares for capital gains tax purposes. But the Inland Revenue said it would not extend the tax year by a day to compensate for the exchange's problems …*
> *The breakdown coincided with news that the exchange had re-opened talks with Deutsche Börse, operator of the Frankfurt financial markets, on a possible merger of their operations." (Financial Times, 2000)*

This 'mere' failure of technology had the power to undermine the board's negotiating position with its potential partner. One can imagine the concern of the board members. The critical issue in both cases is that the business impact was significant and it is 'business impact' that is used as the driving mechanism for IT service continuity management.

A standard approach to IT service continuity involves reviewing the organisation's key business processes to determine the business impact that a disruption would incur. Clearly the disruption is increased as the time outage increases. For each process an amount of time – termed the maximum tolerable outage (MTO) – is determined that

---

[1] Hacktivism can be loosely described as political activism delivered through computer hacking.

represents how long a process would need to be inoperative for a 'disaster' to be declared. In practice, if an outage occurs where the *forecast* time to correct it exceeds the MTO, a disaster would also be declared. This can vary between seconds and months.

Having established what MTO is applicable, for each process a strategy of disaster avoidance and/or disaster recovery needs to be articulated. In many organisations this will be presented in a plan (disaster recovery plan, DRP) which will then be tested through simulation exercises.

Easily said but not so easily done. Many surveys have been conducted into disaster recover planning and the results show a consistent low level of adoption of planning activities (Ernst and Young, 1999; Musson and Jordan, 2000; CFS, 2002; IMJ, 2003; Information Week, 2003; Khanna, 2004; Sheikh, 2004) except in critical industries such as banking (Marlin, 2004). With requirements for BCP now included in the listing rules for the New York Stock Exchange and similar regulations elsewhere, it is anticipated that there will be greater take-up in future. However the performance of IT service continuity activities has not been widely researched. Before developing the research model, we discuss the relationship between business continuity and IT continuity.

Business continuity and IT continuity

Some industries are information intensive (Porter and Millar, 1985) and their dependence on IT is such that high levels of protection are necessary. Developments such as duplicate data centres, duplicate telecommunications providers and power supplies, synchronous replication of data and processes, automatic fail-over systems and frequent testing are part of their stock-in-trade. This is demanded in some industries by the regulators. In order to maintain a banking licence, banks must provide their customers with a very high level of access to their funds. Computerised exchanges, such as those now operating in deregulated electricity markets, must operate at all times, so that power purchases can be made. Airlines and online retailers don't have 'business hours' as their customers are located around the world – so their business must be 'always on'. In addition we have the telecommunications companies, electricity suppliers and other utilities, whose customer base includes these businesses as well as critical community infrastructure such as hospitals and

police services. For these organisations, business continuity intimately includes IT continuity.

It also happens that, in many organisations, the expertise, skills, knowledge and interest of continuity matters are with the IT staff. The early mainframe technologies were so vulnerable and far behind today's reliability standards, that the processes of backing up, logging transactions, and carrying out restore operations were routine even in the 1960s. Today's systems are vastly more complex and have greater networks of dependencies, but the skill set of IT staff has grown to accommodate them. This increase in complexity may be mirrored in some aspects of the supply chain, but most parts of the organisation have not changed in a parallel manner. Thus many organisations look to the IT function for expertise in the area of business continuity, often without recognising it explicitly.

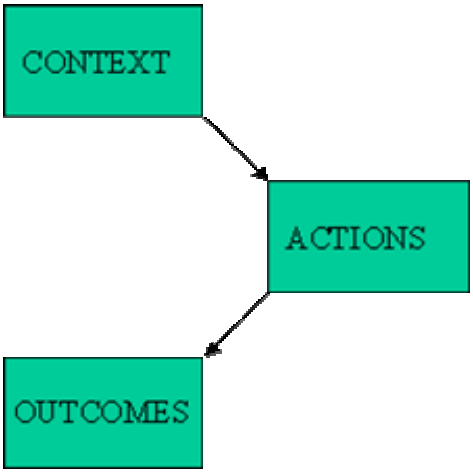
RESEARCH MODEL

Much of the activity in the domain of business continuity is based on professional practice and little research has been published. As a starting point, this paper uses a generic management research model that features in research methods texts. The model is one of implied rational decision-making, based on assessment of the situation. Consequences of those decisions are then apparent at a later time. This model is illustrated in Figure 1.

In the generic management research model, the context of the management decisions and actions are first established. The (rational) manager then chooses actions and makes decisions based on the established context. Results of the actions are observable, typically at a later date and are described as outcomes.

This model ignores the interaction and feedback that takes place in a real environment or more realistic situations where actions are negotiated in a setting that may change the context, and then choose appropriate actions. It is a simple model, even simplistic, but the need is for a model that can be enhanced as research accumulates.

For our research, 'context' becomes the continuity risk environment for the organisation, 'actions' refers to management actions in IT service continuity, and the 'outcomes' will be IT service continuity performance indicators, which are described in the subsequent sections. Thus the IT service continuity research model is shown in Figure 2.



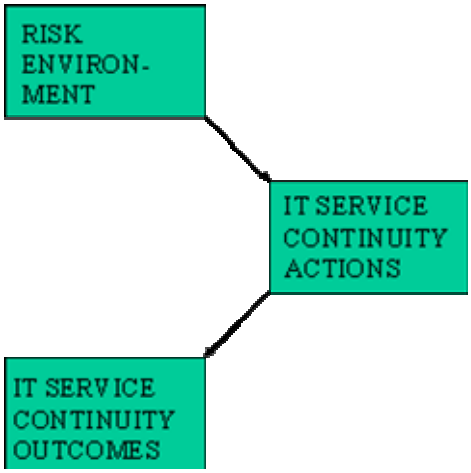


Figure 1 Generic management research model Figure 2 The IT service continuity research model

The risk environment for the organisation

Organisations that are in riskier environments, whether from internal or external sources, would be expected to take greater preparation to counter those untoward events. There are many approaches used by risk managers and IT service continuity professionals. One approach requires the organisation to identify its business processes and examine the vulnerability of each of these. The vulnerability of processes is summarised in a matrix of the likelihood of the loss of the process together with the consequence of that loss, demonstrated in Figure 3.

This approach is often known as a 'business impact analysis', where the impact to the business of a range of foreseeable events is assessed. IFAC (1999) uses a 'risk map' to represent this assessment. Such diagrams can be readily incorporated into presentations to senior management and board members.

Figure 3 Vulnerability matrix for business impact analysis

Factors that add to the risk environment include:

- Pressure from regulators
- Vulnerability caused by 'single points of failure' – key resources that are not duplicated
- Complexity of the organisational environment
- Lack of internal controls, security and senior management oversight
- External hostile parties – hackers, fraudsters, thieves, vandals
- Systems and components with low reliability performance

In this paper we report on a study where a variety of assessments were made of the organisation's risk environment. Managers were asked to specify an MTO, as well as the impacts of loss of computer facilities in terms of recovery.

IT service continuity management actions

The range of actions available to managers fall into few categories: mitigate, insure, ignore, plan and test. Dealing with the simplest first – for vulnerabilities that appear in the lower left hand corner of the asset vulnerability matrix (Figure 3), where both the likelihood and consequence are low, it may well be satisfactory to ignore the issue and accept the risk. The failure of a monitor on a user's system may be just such a risk. Other systems may be able to be out of action for a week without disrupting the business. Parts of the organisation's facilities could similarly be out of action without jeopardising continuous operations.

A common response to more serious risks is to mitigate them, either reduce the likelihood or reduce the consequence (or both). We mitigate the risk of a hard disk crash by carrying out a backup or by purchasing more robust hardware, certified to a high standard. The choice to mitigate will be based upon the likelihood and consequence, when held up against the cost of mitigation. Another method of mitigation is to transfer the risk to another party. Outsourcing a data centre transfers the downtime risk to the vendor, leaving the organisation with the business impacts only, not the hardware costs.

Insurance is the most direct form of risk transfer. In this case the insurance company will provide a benefit that compensates for the negative consequences. Clearly the

insurance company intends to make a profit, so the expected payout would normally be less than the premium. The issue for the organisation is that it is the absolute loss that needs to be mitigated, even though the expected loss is actually increased. This issue is faced by homeowners who insure their property against fire loss, with probability p, for $100,000, say, for a premium that represents more than the expected loss ($100,000 x p). Insurance costs, however, are real costs, while the misadventure has only a probability of occurrence and the loss may never occur.

The final IT service continuity management actions – planning and testing – are normally considered together and form part of a wider business continuity plan. Such BCPs should deal with, *inter alia*, all the IT service continuity risks that are significant and outline what actions are supposed to take place in those eventualities. Tests are undertaken to verify that the planned action is achievable and enables the organisation to resume business. Tests also perform the important function of keeping IT service continuity in the consciousness of the people liable to be affected. Plans are widely derided – gathering dust on a shelf; never examined after being written; costly and impractical – but represent the only assurance to senior management that the organisation has any level of preparedness. Without testing, plans are in danger of meeting the statements of their detractors. Testing reveals weaknesses in plans and allows their revision.

In this study many questions concerned the IT service continuity actions but the focus was on the plans. How complete they were, how recently modified or adopted, whether tested or not, whether approved by senior management. Together these questions should give a comprehensive assessment of the management preparedness and competence in IT service continuity. Managers were also asked to give a summary assessment of the state of their overall preparedness.

IT service continuity outcomes

Professional practice concentrates on two key performance areas:

- resilience – the ability to withstand unwelcome events, and building such capacity, and
- recovery – the ability to come back after a forced outage.

Resilience can be likened to our personal health issues of ‘having our shots’, ‘getting health checks’, ‘keeping fit’ and ‘keeping our resistance up’. For a business

organisation intent on building IT service continuity resilience, it must work to identify single points of failure and remove them; it must monitor the reliability of components and replace the inadequate, and so on. With a high level of resilience, more disruptions and failures can be tolerated without degradation in business services. Resilience in terms of hardware, telecommunications connections, power supplies and other physical assets can be assessed in a straightforward manner, however the issue to the organisation's customer is one of service delivery, and other factors are important. Thus assessing resilience in terms of the delivery of services can be much more difficult than for infrastructural components.

Recovery is concerned with bringing back the organisation to an acceptable performance level, in particular the costs and time involved, although for many organisations, simply being able to recover – at all – is in itself the necessary achievement. It could be argued that recovery can only be measured when there is some significant event. However, the realistic situation is that outages of a minor nature are frequently occurring. Power outages are very common, as are telecommunications breaks. Increasingly today, we find that network outages due to viruses, worms and the like, are also routine. While simple breaks are everyday, there are usually distinguishing features of each event, and the duration is seldom known at the outset. Thus those concerned must bring into action their procedures for dealing with extended breaks. Most large IT installations routinely log all such service breaks and record their durations. It is uncommon that business performance degradation, e.g. customer service level, is also recorded during these episodes. This study asked organisations about their experience of outages and their recovery performance.

A third component of business continuity outcomes is not part of the standard professional practice. This concerns the business benefits obtained by the very process of carrying out IT service continuity assessment exercises. The close examination of the importance and vulnerability of business systems and processes may bring about a better understanding – revealing the potential for improvement, rationalisation or redesign. These outcomes from business continuity planning are the current benefits. These have been investigated independently by case studies but are difficult to approach in a survey methodology, due to their distinct individual nature.

In this study the outcomes were assessed by asking managers for the perceived resilience of their organisations and the confidence that they would be able to recover in an acceptable time.

Hypotheses

Effect of risk on planning

It is to be anticipated that organisations that are in a riskier environment, from whatever causes, will be more likely to be carrying out IT service continuity planning. In this study the measures of environmental risk are the maximum acceptable outage (MTO), facility loss assessments and ownership of mission critical systems. An overall 'continuity risk assessment' was also requested from the participants.

There were many measures of IT service continuity management actions: existence of plans, age of plans, test currency of plans, budget for business continuity, and management responsibility level for business continuity, but in the end the greatest discrimination between organisations was found for the overall status (from 'documented and approved' to 'no plan') of the IT continuity plan and the business continuity plan. These were summed as 'status of continuity plans'.

Thus we expect higher levels of risk to lead to higher levels of management action, in particular:

- A shorter MTO is expected to lead to higher status continuity plans
- Ownership of mission critical systems is expected to lead to higher status continuity plans
- Higher risk facilities are expected to lead to higher status continuity plans
- A higher 'continuity risk assessment' is expected to lead to higher status continuity plans.

Effect of planning on outcomes

It is to be hoped or expected that those organisations with better planning and preparedness will fare better during a disturbance – assuming that they have the same risk level. We have considered the measurements of management action above, which leaves only the outcomes to be assessed. We expect that organisations with more

planning activities will have higher perceived resilience and better (shorter) recovery capabilities, in particular:

- Organisations with more planning activities are expected to have higher perceived resilience
- Organisations with more planning activities are expected to have better tested continuity assessments.

In terms of the graphical model in Figure 2, this can now be annotated with the variables that are obtained in the investigation. This is shown in Figure 4.

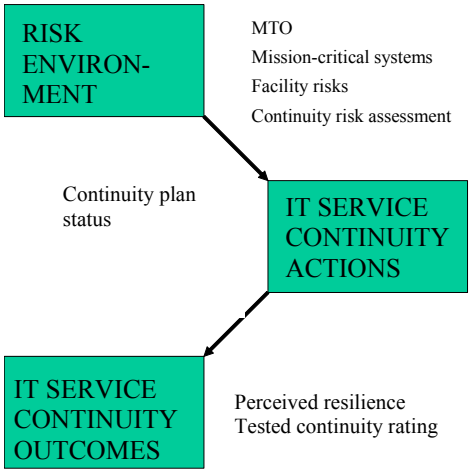


Figure 4 The operationalised model

METHODOLOGY

The survey instrument[2] was developed by considering a range of documents; sources included Australian Standard AS4444 (Standards Australia, 1999), Coopers & Lybrand (1992), Ernst & Young (1996), FEMA (1996), Hardy (1992), Higgins and Tilley (1998), Hiles and Barnes (1999), Musson and Jordan (2000) Internal Auditor (1997), Kearvell-White (1996), Maslen (1996), NCC (1994, 1996), Survive (1996) and Tilley (1998). It addressed other background data as well as the items being reported here. This enabled each document to be internally verified for consistency and telephone follow-up of any apparent inconsistencies.

[2] Available from the author's website.

This survey focussed on Australian Federal Government organisations, including Department, quasi-independent Agencies and public Corporations (with majority Government shareholding). The mailing list was derived from the Australian Commonwealth "Gold Book" – a directory that is published regularly and available online (www.directory.gov.au). Small and very small agencies were excluded from the study, as it would be unlikely that they would have significant IT resources or dependency. This reduced the population surveyed to 120 organisations.

Given that the instrument included wider business continuity issues (not just IT services) it was decided to address the survey to the CEO[3] of the organisations. This reflects the view that business continuity planning (and thus the survival of the organisation) is a matter of corporate governance. A letter was produced, which was designed to obtain the commitment of the addressee; it was sent to the CEO and was individually signed. It asked the recipient to pass on the enclosed questionnaire to the manager concerned, and also asked that the recipient completed a notification form, giving the name of the person to whom the questionnaire had been passed. The notification form also asked the CEOs whether they would like a copy of the survey report. The survey was approved by the University's Human Ethics Committee.

Response and validity

The survey response rate was over 20% which can be regarded as adequate for this paper as it concentrates on model development, but limiting the ability to generalise the conclusions. Factors contributing towards the low rate include the size of the questionnaire and the then-current Y2K overload – the number of questionnaires being requested of senior managers for Y2K purposes. Analysis of non-response showed that they did not exhibit systematic patterns. The overall results were also very similar to the earlier study (which had a higher response rate), increasing the author's confidence that the results were reliable.

[3] The title of chief executive officer is rare in government organizations, frequently the title Secretary is used. We use the term CEO in a generic sense.

RESULTS

In this section we look at the results under each of the three major categories: risk environment, business continuity actions and business continuity outcomes[4].

[4] Full tabulation of all the variables in the questionnaire are available on the author's website.

Risk environment

MTO values varied from less than 8 hours to more than seven days in spite of the fact that almost all the organisations had 'mission-critical systems'. The facility risk variables:

- consequence of loss of IT facility
- external visibility of services
- consequence of 7day stoppage
- consequence of one month building access loss,

were all found to be highly correlated with each other. An aggregate variable "Impacts" was created by adding the values for the four variables. This was itself highly correlated with the 'continuity risk assessment' variable.

Continuity actions

'Continuity plan status' was a newly-created aggregate variable representing the sum of the business continuity plan status and the IT service continuity status. Many other data items, such as age of plans, extent of testing, level of management responsibility in the organisation, were assessed for their contribution to the analysis but were rejected. In many cases there was insufficient data, or insufficient variability.

Continuity outcomes

The 'perceived resilience' variable only exhibited small variability. The concept 'resilience' had been defined in the questionnaire but perhaps it was not sufficiently clear to the participants. A summative evaluation of the organisation's entire continuity planning and testing achievement was the final question on the questionnaire. It was strongly correlated with attributes that reflected intense activity (e.g. full intrusion detection systems, application mirroring). This 'tested continuity rating' exhibited sufficient variability to be used in analysis.

ANALYSIS AND DISCUSSION

Relationship between environment and continuity actions

No relationship was found between two risk environment variables – MTO and ownership of mission critical systems – and any of the business continuity action

variables. However both the facility risk assessment and continuity risk assessment were strongly correlated with continuity plan status. No other continuity action variable was associated with any of the environmental variables. Clearly the extent of some risk factors alone is not sufficient to warrant continuity planning, but requires other aspects of the organisational setting, such as budget capacity and management willingness. While both 'facility risk assessment' and 'continuity risk assessment' were correlated with planning status, the correlation with 'facility risk assessment' was noticeably stronger ($p<0.001$). It could be that the continuity risk assessment was more subjective, and the facility risk questions addressed very specific outages and contingencies, e.g. a building being unavailable for a month.

Relationship between continuity actions and continuity outcomes

Planning status was strongly correlated ($p<0.001$) with tested continuity rating. Inspection of many of the cross-tabulations of planning variables with response variables showed apparently noticeable trends but the sample size was insufficient to find other convincing results. Perceived resilience was not correlated with the planning variables, but the issue of the participants' understanding of the term 'resilience' has been addressed above.

Thus the analysis showed that both stages of the model were supported: risk environmental factors are strongly correlated with selected planning actions, which are in turn strongly correlated with outcome variables.

CONCLUSIONS

The generic management model has proven useful in establishing a foundation for cumulative development of research in the area. The proposition that a riskier environment leads to greater planning activity which in turns leads to a positive assessment of readiness is supported. It is concerning that many of the questionnaire components were found to be unrelated to the broad measures at each stage. Clearly simple statistical measures, such as correlation, are insufficient to deal with the complexity of one highly-rated risk causing an organisation to engage in extensive planning, testing and preparedness, when many other risk variables may have low scores. Techniques relying on means and variance, with underlying assumptions of normality could be inappropriate in such settings.

Research is continuing with simultaneous attempts to strengthen the summative variables at each stage of the model, gather more data, and revise the data analysis procedures.

This paper builds on and revises an earlier model (Jordan, 2003); it includes new data and completely new analysis.

ACKNOWLEDGEMENTS

This research was generously supported by Hewlett-Packard Business Continuity Services (Asia-Pacific) and SMS Management & Technology (Canberra, Australia). The author would like to express his gratitude to those involved.

REFERENCES

AFR (2004) "SCO rides out the Mydoom storm", Lebihan, R., *Australian Financial Review*, 4 February

BSI (1999) *BS7799 Part 2: Specification for information security management systems*, British Standards Institute, London

CFS (2002) "Business continuity research highlights problems", *Computer Fraud & Security*, May, p.3 (editorial)

Coopers & Lybrand. (1992) *Corporate Security and Contingency Planning*, Sydney

Ernst & Young (1996) *Information Security Survey 1996*, October 1996, New York

FEMA (1996) *Emergency Management Guide for Business and Industry*, Federal Emergency Management Agency, September 1996, Washington

Financi al Times (2000) "Glitch halts share trading in London" *Financial Times*, London, 6 April.

Garigue, R. and Stefanin, M. (2003) 'Information Security Governance Reporting', *Information Systems Security*, Sep-Oct., 36-40

Hardy, K. (1992) 'Contingency Planning', *Business Quarterly*, Spring 1992, **56**, 4, 26-28

Herbane, B., Elliott, D. and Swartz, E. (2004) 'Business continuity management: time for a strategic role?', *Long Range Planning*, 37, 435-457

Higgins, Y and Tilley, K. 1998. Business continuity plans tested by fire Down Under. *Business Insurance* (32) 26. p23. June 29.

Hiles, A. and Barnes, P. (1999) (eds.) *Business Continuity Management*, Wiley, Chichester

Holzinger, A. (2000) Information security management and assurance, *Information Systems Security*, May/June, 32-39

IFAC (1999) *Enhancing shareholder wealth by better managing business risk, Study 9,* International Federation of Accountants, New York, June.

Information Week (2003) 'Behind the numbers: business continuity slides down the priority scale', Jan 13, 2003, p.61

Internal Auditor, 1997. Disaster recovery plans not a priority. *The Internal Auditor*. December.

IMJ (2003) "Few organisations have effective continuity plans", *Information Management Journal*, May/June, p.7

Jordan, E. (2003) "Performance Measures in Business Continuity", Proceedings, 14th Australasian Conference on Information Systems (ACIS), 26-28 November

Jordan, E. and Silcock, L. (2005) *Beating IT Risks*, Wiley, Chichester, UK

Kearvell-White, B. (1996) "National (UK) Computer Security Survey 1996", *Information Management & Computer Security*, **4**, 3, 3-17

Khanna, P. (2004) "Blackout shines light on need for business continuity plan", *Computing Canada*, Sep. 10 2004, p.16

Lindup, K. (1996) 'The role of information security in corporate governance', *Computers & Security*, 15, 477-485

Markus, M. (2000) "Towards an integrative theory of risk control", in R. Baskerville, J. Stage and J. DeGross (eds) *Organisational and Social Perspectives on Information Technology*, Boston, MA, Kluwer, 167-178

Marlin, S. (2004) "Disaster recovery spending on the rise", *Information Week*, Aug. 9 2004, p.26

Maslen, C. (1996) "Testing the plan is more important than the plan itself", *Information Management & Computer Security*, **4**, 3, 26-29

Musson, D. and Jordan, E. (2000) *Managing for failure: the Macquarie University survey of business and computer contingency planning in Australia*, Macquarie Research Ltd, Sydney

NCC (1994) *Information Security Breaches Survey 1994*, National Computing Centre, UK

NCC (1996) *Information Security Breaches Survey 1996*, National Computing Centre, UK

Peppard, J. and Ward, J. (2004) "Beyond strategic information systems: towards an IS capability", *Journal of Strategic Information Systems*

Porter, M.E. and Millar, V.E. (1985), "How Information gives you Competitive Advantage," *Harvard Business Review*, vol. 63, no. 4, pp. 149-160

Posthumous, S. and von Solms, R. (2004) 'A framework for the governance of information security', *Computers & Security*, 23, 638-646

Sheikh, F. (2004) "Disaster recovery plans must evolve as risks change", *Computing Canada*, March 26, p. 10

Standards Australia (1999) *Information security management,* AS/NZS 4444:1999, Sydney

Survive! (1996) *Survive! Survey of disaster recovery*, Survive!, London

Tilley,K. 1998. Fire shows disaster plans wanting; major industries in Longford Australia suffer growing production losses. *Business Insurance* (32) 40. P57. October 5

Von Solms, B. (2001a) 'Corporate Governance and Information Security', *Computers and Security*, 20, 215-218

Von Solms, B. (2001b) 'Information Security – a multidimensional discipline', *Computers and Security*, 20, 504-508

Williams, P. (2001) 'Information Security Governance', *Information Security Technical Report*, 6, 3, 60-70