STRATEGIC SYSTEMS? ONLY WHEN THEY WORK!

Ernest Jordan
David Musson
Macquarie Graduate School of Management
Macquarie University
Email: Ernest.Jordan@mq.edu.au

ABSTRACT

This paper presents the results of a sample survey of Australian organisations' approaches to business and information technology (IT) contingency planning. The survey was undertaken because there was a perception that coping with disaster is a much neglected aspect of management in Australia. It is an exploratory study that seeks to establish the current levels of awareness and preparedness. The findings reveal that most organisations are inadequately prepared and fail to take the issue seriously. Business continuity is not rated as a high priority.

KEYWORDS

EK08 Disaster plans, **EK** IS Security, **EL08** IS Risk Management

INTRODUCTION

The late 1980s saw a dramatic rise in the perceived importance of strategic planning for IS and IT. Several surveys of North American MIS managers (such as Dickson *et al.*, 1984; Hartog and Herbert, 1986; Lederer and Mendelow, 1986; Brancheau and Wetherbe, 1987) showed strategic planning high on the list of key issues, having risen rapidly to that prominence. In part it was fuelled by the necessity for many organisations to think in terms of strategic applications because their customers, competitors, suppliers and others in the world around them were doing the same (Earl, 1989). It became a competitive necessity for an organisation to carry out some form of planning if its competitors were themselves searching for opportunities for competitive advantage. The external stimulus provided a focus for the changes that were finding their way into the organisation.

Security and Control

However a falling star during this era was security and control. Brancheau and Wetherbe (1987) show 'security and control' as only ranked 18th in the list of key issues. Perhaps 'everyone knew' what they had to do in order to keep systems secure, and to maintain control over the IT environment. By the time of the most recent (1994-5) survey in the series (Brancheau, Janz and Wetherbe, 1996), security and control has disappeared completely. Interestingly, the beguiling 'competitive advantage' has sunk to 18th place so we can anticipate that it too will disappear from future surveys. However the top item in the 1994-5 survey is 'Building a responsive IT infrastructure' which reflects the demanding challenge of constructing a reliable and responsive framework for connectivity and applications. We would argue that reliability is an integral feature and that 'security and control' is implied.

If IT applications are indeed competitive or strategic or critical to business needs, then one would anticipate that establishing a high level of operational reliability for such systems is imperative. Part of this challenge concerns what happens in an emergency or disaster, a topic usually known as IT contingency planning or disaster recovery planning.

One way of demonstrating both the real level of importance of IT to an organisation, including its strategic or competitive potential, and the gap between the 'headline' IT and the operational reality, is to consider the cinderella issue of security and control. If IT truly is of critical importance to an organisation, if systems are 'strategic', then it certainly needs to be safeguarded; perhaps the systems simply aren't critical or strategic. On the other hand, it could be a matter of a difference between what is said and what is done, what Argyris called a difference between 'theory espoused' and 'theory in use'. Perhaps IT is *critical* or *strategic*, but we *just don't* do what we know we should, mimicking the individual's responses to home insurance and the like.

Security is certainly not glamorous; CIOs would not allocate this issue to their 'best and brightest'. It is, however, a challenge for the organisation. Given that disasters do happen, we wished to examine the preparedness of organisations to deal with them. Particular issues include the level of preparedness and the personnel responsible for it.

We have also found links in the literature between IT contingency planning and business contingency planning. While IT may be a key operational enabler, the business itself unquestionably would need to be able to continue - its very existence should be safeguarded. In this context we wanted to find out to what extent IT and business planning were coordinated, whether the same people were involved and which of these was more widespread.

RESEARCH QUESTIONS

The research addresses three key areas: the nature of experienced contingencies, the extent of planning, and the operationalisation of the plan. The overall aim is to find out whether Australian businesses are taking the risks to their businesses and IT seriously. From this we can establish the level of awareness and preparedness, and plan interventions such as education, workshops and self-assessment schedules.

Experiences

There is a wide range of contingencies that may be experienced, some of them common (such as power failure and communication line failure) and others extremely rare (such as extensive fires, major accidents, or bombs). We wished to establish benchmarks for the frequencies of the most common events. The level of occurrence can be expected to be related to the extent of computerisation so this needed to be monitored.

Plan Formulation

The simplest, clearest and most widely agreed strategy to deal with contingencies is to have a plan. There are many standards published in Australia that cover aspects of storage, protection and documentation of IT assets, but the umbrella document is the Australian Standard AS4444:1996 Information Security Management (Standards Australia, 1996). We were concerned to find out whether organisations had created plans and what those plans contained. In particular, to determine the extent to which the plans covered items mentioned in the standard.

Plan Operationalisation

Putting a plan into operation does not require a disaster to happen. Testing and rehearsing aspects of the plan, educating and training those with special responsibilities, such activities are to be expected in a prepared organisation. Minor contingencies need to be dealt with frequently and these can reveal shortcomings in the plan. The study examines the evidence that the plans are operational.

Hypotheses

Since this investigation is attempting to determine current levels of preparedness against conventional advice, such as the Australian Standard, it was not considered necessary to develop comprehensive *a priori* hypotheses. It is the aim of the research to enable hypotheses to be formed for future work and to establish a reference point for future studies.

METHODOLOGY

Given that the overall aim is to establish an indication of the Australia-wide level of preparedness, it was decided that a survey was necessary. Furthermore, the majority of the concepts and issues related to contingency planning are well understood and may reasonably be answered in a questionnaire format. The study questionnaire was addressed to the CEO of the selected organisations, to be forwarded to the 'person responsible'. A reply coupon from CEOs specified the contact person; most participants requested a copy of the final report.

In defining the population to be the target of the survey, it was decided that Australian state and federal government departments and agencies would be excluded. There were two main reasons for this: it was anticipated that the overall level of preparedness would be high because of mandatory controls, and secondly, we expected some reluctance to respond from such organisations. We further restricted ourselves to Australian organisations with significant computer configurations (more than 20 users).

Sample selection

The mailing list was based upon the MIS 4000 database of Australian and New Zealand computer users (Strategic Publishing, 1996). This database lists 4169 computer users. 19% (or 792) of these were in New

Zealand, 16.4% (or 684) of these were in the public service and 5.7% (or 238) were IT suppliers. Excluding these gave a total of 2455 users. 31 other organisations were also excluded; mainly holding companies whose operating companies were also listed. This left a total of 2424 organisations.

A stratified random sample of organisations was selected, representing some 10% of the larger industry groups and some 20% of the smaller industry groups.

Industry	**Size**	**Sample**	**Industry**	**Size**	**Sample**
Manufacturing	822	82	Mining & agriculture	138	28
Wholesale	265	27	Services	318	33
Retail	121	23	Electricity & gas	63	11
Construction	202	19	Transport	70	13
Finance	393	41	Personal services & tourism	32	6
Total				**2424**	**283**

Table 1: Sampling population and sample sizes

Questionnaire Development

The questions in the questionnaire can be divided into several groups. These are:

- **Introductory questions:** organisation size, and computer configuration.
- **Service interruption questions:** effects of loss of systems, frequency of interruptions, duration and cause of failures, and tolerable out-of-service times.
- **Backup questions:** intended to build up a picture of the backup procedures and the experience in taking and restoring backups.
- **Contingency planning questions:** seeking to establish the degree of planning in place, staff responsibilities and policies.

INITIAL TABULATIONS

Detailed tabulations of all questions as well as the questionnaire are published elsewhere (Musson and Jordan, 1997). The response rates were not significantly different across the industry sectors. The overall response rate was just over 25% — acceptable for such a demanding and invasive questionnaire. The responses received to a selection of the questions in the survey are set out below.

	Number of employees	
No. of employees	Count	Percentage
1-49	9	12.7
50 -199	22	31.0
200 - 499	17	23.9
500 +	22	31.0
No answer	1	1.4
Total	71	100.0

Table 2: Responses by number of employees

Table 2 shows that the responses demonstrate a reasonable coverage of the range of organisational sizes. There is no excessive emphasis on any size category.

Type	Number	% of Responses
Mainframe	17	23.9
Midrange	47	66.2
Client/Server	51	71.8
LAN/networked PCs	69	97.2
Standalone PCs	49	69.0

Table 3: IT holdings of Respondents

Multiple responses were anticipated and received. This causes some anomalies to counts in some of the following questions.

	M/frame	loss	Midrange	loss	Server	loss	Network	loss	PC	loss
	Count	%	Count	%	Count	%	Count	%	Count	%
No answer					1	1.9			1	2.0
Critical	12	70.6	31	66.0	24	45.3	12	17.4	1	2.0
Very disruptive	3	17.6	13	27.7	14	26.4	28	40.6	3	6.0
Disruptive	2	11.8	2	4.3	13	24.5	19	27.5	20	40.0
Minor inconvenience			1	2.1	1	1.9	10	14.5	23	46.0
No inconvenience									2	4.0
Total	17	100.0	47	100.0	53	100.0	69	100.0	50	100.0

Table 4: Effect of loss of Computer Services

Table 4 shows that the effect of loss of mainframe, midrange and server systems is typically regarded as very disruptive or critical. Network failure is not quite as critical and the failure of standalone PCs are not generally regarded as more than 'disruptive'.

	Experienced interruptions	
	Count	%
No	18	25.4
Yes	51	71.8
Don't know	2	2.8
Total	71	100.0

Table 5: Critical service interruptions

Length of interruption	Count
less than 1 hour	483
1 to 4 hours	161
4 to 24 hours	58
1 to 3 days	9
4 days to 1 week	1

Table 6: Length of interruptions

Table 5 indicates that interruptions to critical services are not unusual, with the majority of organisations experiencing this during a period of two years. The detail provided in Table 6 is substantial, with each organisation experiencing and reporting some ten interruptions on average.

Type	Count	%
Hardware failures	115	29.3
Software failures	153	39.0
Power failures	61	15.6
Accidents	22	5.6
Other causes	41	10.5

Table 7: Cause of service interruptions

	Count	%
No answer	1	1.4
< 8 hours	28	39.4
8 - 24 hours	21	29.6
1 - 2 days	16	22.5
2 - 7 days	4	5.6
> 7 days	1	1.4
Total	71	100.0

Table 8: Longest tolerable “out-of-service” time for most critical applications

Table 7 shows that hardware and software failures together comprise the majority of failures experienced. "Disasters" are indeed rare. Table 8 shows that some 40% of organisations regard up to 8 hours as the largest tolerable out of service time. This gives an absolute size to the qualitative judgements such as 'critical' or 'disruptive' shown in Table 4 and elsewhere.

	Count	%
Yes, time acceptable	34	47.9
Yes, time unacceptable	8	11.3
No estimate of time	23	32.4
Could not recreate data	2	2.8
Don't know	3	4.2
Total	70	98.6

Table 9 Estimate of time to recreate data if backup failed[5]

More than 50% of organisations are exposing themselves to risks in this area. An estimate of the time to re-create data from scratch is needed in any comprehensive plan.

	Company has plans for:	
	Count	%
Complete business operations including IT	14	19.7
IT only	23	32.4
Neither business nor IT	34	47.9
Total	71	100.0

Table 10: Holding of contingency plans by Australian companies

Table 10 shows that only one fifth of organisations have established plans for both the business and for IT. Almost half of the organisations have no contingency plans at all. Over 30% of the organisations only have contingency plans for IT.

	Business plan duration		IT plan duration	
	Count	%	Count	%
< 1 year	4	5.6	6	8.5
1 -2 years	7	9.9	11	15.5
3 - 5 years	2	2.8	13	18.3
> 5 years	1	1.4	4	5.6
No plan	53	74.6	34	47.9
Being developed	4	5.6	2	2.8
Total	71	100.0	70	98.6

Table 11: Length of time the plans had existed

Only three organisations have had business contingency plans for more than two years. IT plans are much better established. This question confirms the answers given in previous questions about the general absence of plans.

[5] In several tables multiple responses and missing or qualified answers cause different totals

	Business plan missing		IT plan missing	
Reason	Count	%	Count	%
No answer	4	6.9	1	2.6
Necessary but low priority	24	41.4	20	52.6
Not considered necessary	4	6.9	1	2.6
Not considered	4	6.9	1	2.6
Insufficient resources	11	19.0	11	28.9
Don't know	7	12.1	2	5.3
Being developed but not ready	4	6.9	2	5.3
Total	58	100.0	38	100.0

Table 12: Reasons for not having produced plans

Overwhelmingly the reason for not having contingency plans is their perceived low priority, together with the resource requirement needed to produce plans.

	Last test of business plans		Last test of IT plan	
	Count	%	Count	%
No answer			1	1.4
During the last year	3	4.2	25	35.2
1 - 2 years ago	2	2.8	5	7.0
Over 2 years ago	2	2.8	5	7.0
Not tested	8	11.3	12	16.9
Don't know	49	69.0	22	31.0
No plans	7	9.9	1	1.4
Total	71	100.0	71	100.0

Table 13: Time of last testing of contingency plans

Testing of business contingency plans seems to be a patchy business, with most organisations unable to answer. IT plans were recently tested in roughly one third of organisations.

	Day-to-day responsibility		Implementation responsibility	
	Count	%	Count	%
MD / chief executive	0	0.0	11	14.1
Main board member	3	4.0	7	9.0
IT manager	44	58.7	37	47.4
Line manager	12	16.0	8	10.3
Staff member	2	2.7	5	6.4
No plans	13	17.3	10	12.8
Total	74	100.0	78	100.0

Table 14: Responsibility for plan implementation in an emergency

Table 14 shows that more than half of organisations give responsibility to the IT manager for the plans, both business and IT. This then leaves open the question, hopefully to be investigated in the future, of why this is the case. The implementation of plans in an emergency is also frequently the responsibility of the IT manager, although more senior managers are also cited.

	Count	%
No answer	2	2.8
Yes, completely confident	11	15.5
Yes, believe they will	33	46.5
They probably will	11	15.5
Unsure that they will	13	18.3
Qualified answer	1	1.4
Total	71	100.0

Table 15: Level of confidence that plans will ensure survival of the business

It is our belief that only one of the answers in Table 15 is acceptable, yet only 15% of organisations gave it.

DISCUSSION

Highly significant extracts from the survey show that:

Just 20% of Australian organisations have disaster recovery plans that cover their entire business operations, and 50% have no plans at all.

38% of organisations that have a maximum of 24 hours out-of-service time for their computer systems and have no plans to deal with a longer stoppage.

In most cases, the IT manager is responsible for the *company* disaster recovery plans.

These headline figures show that planning for recovery from disaster is still a neglected subject in Australian boardrooms. Whilst Australian business has been relatively free from attack by terrorists and other malevolent people, it is still vulnerable to damage from fire, flood and earthquake, and to accidental damage from a wide variety of sources. Failure to plan for unscheduled interruption to the business is thus a serious failure in corporate governance. "Very few board chairmen, presidents or general managers would run a business without insurance. For some reason, they have yet to look at disaster recovery planning in that light" (Rothstein, 1988).

Contingency Planning

Before beginning an analysis of the survey results, it is perhaps appropriate to clarify the term "contingency planning". Hardy (1992) proposed that all events that occur at an organisation could be described in the dimensions of predictable / unpredictable and controllable / uncontrollable. The Federal Emergency Management Agency in the US uses the term "emergency" to describe these unpredictable, uncontrollable events. It defines emergency as:

"Any unplanned event that can cause death or significant injuries to employees, customers or the public; or that can shut down your business, disrupt operations, cause physical or environmental damage, or threaten the facility's financial standing or public image." (FEMA, 1996)

The same document makes the point that the term "disaster" is not used in the document because "it lends itself to a pre-conceived notion of a large-scale event, usually a 'natural disaster'. What might constitute a nuisance to a large industrial facility could be a 'disaster' to a small business" (FEMA, 1996). In our survey, we were looking at the degree of planning against emergencies in Australian organisations.

The Issues

Two management issues are clearly evident in the results of the survey. These are: the number of companies without contingency plans and other key policies; and the question of who is in charge of plans, both day-to-day and in an emergency. These are dealt with in turn below.

Plans and Policies

Question 7 of the survey asked what was the respondents' longest tolerable "out-of-service" time for critical applications and/or services; the answers were noted in Table 8, above. Sixty-eight percent of respondents cannot tolerate breaks in service of a day or less, and over 90% could not tolerate breaks of 2 days or less. These figures would certainly support the case for contingency planning amongst the majority of Australian organisations; it is inconceivable that any but the smallest organisation could completely re-create their IT systems within 24 hours without a plan. It would be even less likely that they could restart their complete business in that time without a plan.

Holding of plans

The main findings were:

- Nearly half of all organisations have no formal plans for disaster recovery of their business and their IT.
- Less than 20% of organisations have full business contingency plans; of these plans, 57% have never been tested.
- 53% of organisations have IT plans. Two thirds of these IT plans had been tested in the last 12 months, but a significant number had not been tested and several were last tested over two years ago.

The detailed results are shown in Tables 10 and 13, above. Note that there are fewer IT plans reported in Table 10 than there are tested plans in Table 13. This suggests that there are informal plans for IT disaster recovery held in organisations.

The low level of testing is as worrying as the low level of plan holding. Clearly a plan that has not been tested is not a reliable plan; the act of testing the plan may well show up omissions in the plan or, for example, faulty safety equipment. One person interviewed during the course of this study instanced the testing of an emergency siren that was found to be not working - it had been installed for five years and never previously tested.

Other surveys of plans holdings

Other surveys in Australia and the UK help to put these figures in context. The Coopers & Lybrand survey (Coopers & Lybrand, 1992) reported that 51% of Australian organisations had computer contingency plans, although their figures included public sector organisations who might be more likely to institute contingency plans. Figures from the UK appear to show that companies there are better prepared for disaster. In 1994, 59% of UK companies polled by the National Computing Centre in 1994 had formal IT plans and this figure rose to 63% when the poll was repeated in 1996 (NCC, 1994; 1996). The Securicor (1996) data security report surveyed 1,741 medium and large UK organisations, and found that 60% of them had IT disaster recovery plans. The Ernst & Young (1996) Information Security Survey for 1996 found that almost 75% of organisations polled (in the US) had an IT disaster recovery plan but 42% of these had not been tested. In general, it is clear that IT management is well aware of the potential for damage to business operation posed by a failing computer system, and makes formal or informal plans for recovery from system failures.

There have been fewer surveys of business contingency planning. Coopers & Lybrand (1992) reported that 39% of Australian organisations had a corporation-wide contingency plan for critical services, although their figures again included public sector organisations. The UK 1996 IBM/Cranfield study (IBM, 1996) found that 35% of private sector organisations had business disaster recovery plans, again suggesting that the UK is rather better prepared, although the figure is still low.

Further analyses of the survey findings on planning

Detailed analysis of our Australian survey figures throws more light on to the state of contingency planning for IT failure. Comparing planning arrangements to the respondents ranking of the effects of loss of their computer services produces the results in Tables 16, 17 and 18. If we restrict analysis to those respondents who regarded their systems as critical to their business operations, 24% of these mainframe respondents, some 32% of mid-range respondents and some 30% of server respondents had no plans of any kind.

Company	Has complete plans	Has only IT plans	Has no plans
Critical	3	5	4
Very disruptive			3
Disruptive			2
Total	3	5	9

Table 16: Planning arrangements against effects of loss of mainframe computer system

Company	Has complete plans	Has only IT plans	Has no plans
Critical	4	12	15
Very disruptive	2	5	6
Disruptive	1		2
Minor inconvenience		1	
Total	7	18	22

Table 17: Planning arrangements against effects of loss of midrange computer system

Company	Has complete plans	Has only IT plans	Has no plans
Critical	6	3	15
Very disruptive		8	6
Disruptive	4	6	3
Minor inconvenience			1
Total	10	17	26

Table 18: Planning arrangements against effects of loss of server system

A breakdown of the companies planning arrangements by their maximum tolerable "out-of-service" time produces the results shown in Table 19, below. Nineteen responses, or 27% of the total, had maximum times of less than 8 hours but no business contingency plans; 26 responses or 37% had maximum times of less than 24 hours, but no plans. Given that a relatively minor fire or explosion could put an organisation out of business for several days, then 37% of Australian organisations are putting their entire business at considerable risk.

Company	Has complete plans	Has only IT plans	Has no plans
Less than 8 hrs	5	4	19
8 - 24 hours	6	8	7
1 - 2 days	2	7	7
2 - 7 days		3	1
More than 7 days	1		
Total	14	22	34

Table 19: Planning arrangements against maximum tolerable out-of-service time

Confidence in planning arrangements

Question 20 asked whether respondents were confident that their current contingency plans would ensure the survival of their business after a disaster. Responses were given in Table 15, above. Less than 20% were unsure that their plans were sufficient but only 16% were completely confident that they were in fact sufficient.

Two further analyses show that many businesses have boundless confidence in their ability to survive a disaster without any form of planning. Table 20, below, shows a comparison between the responses to the question on confidence and the answers on the existence of contingency plans. Almost 60% of the organisations with neither business nor IT plans had some confidence that they could survive a disaster.

Company	Has complete plans	Has only IT plans	Has no plans
Completely confident	3	6	2
Believe sufficient	10	13	10
Probably OK	1	2	8
Unsure sufficient		1	12
Total	14	22	32

Table 20: Planning arrangements against confidence of survival

Table 21, below, shows confidence against the arrangements for temporary computing facilities. Eleven respondents (over 15%) had no alternative arrangements. Ten respondents intended to buy new or used replacements. This is not likely to be an effective strategy for most companies, because of the time lag between the disaster and getting the systems back in service, due to the time taken in sourcing, purchasing, installing and commissioning the replacements.

Confidence:	Complete	Strong	Probable	Unsure
In-house	7	11	2	3
Manuf./ hot site	3	7	1	1
3rd party stand-by		2	1	
3rd party hot site		3	1	
3rd party cold site		2	2	
Buy new/used	1	6	2	1
Reciprocal arr.				1
No arrangement		2	2	7
Total	11	33	11	13

Table 21: Temporary IT arrangements against confidence of survival

Who is in Charge?

The change in emphasis in contingency planning from ensuring an uninterrupted computing service to ensuring the survival of the business has meant that, overseas, the responsibility for planning and management of these plans has moved from the IT Manager to senior line management. This is reflected in the Survive! survey conducted in the UK between April and July 1996 (Survive! 1996). The responsibility for business continuity was held by the IT organisation in only 19% of the 450 respondent organisations, compared to 45% only 18 months before. Our survey showed the IT manager is responsible for day-to-day management of plans in almost 60% of Australian organisations (see Table 14, above) and is responsible for implementation of those plans in an emergency in nearly half of Australian organisations.

Table 22 give valuable insights into the placement of responsibility. For those companies with comprehensive plans, some 29% gave their IT manager responsibility for implementing plans in an emergency but over 64% held the IT manager responsible for the management of the plans. For those companies with only IT plans, 70% of them gave the IT manager responsibility in an emergency. This suggests that IT is still seen as the owner of the company's disaster recovery plans in Australia. It is noticeable that those companies with comprehensive plans mostly (57%) appointed a director to take charge in an emergency.

	Day-to-day responsibility			Implementation responsibility		
Company has	complete plans	only IT plans	no plans	complete plans	only IT plans	no plans
MD/ chief executive				6	2	2
Main board director	1	1	1	2	3	2
IT manager	9	19	16	4	16	15
Line manager	3	2	3	1	1	1
Staff member	1		1	1		4
No plans			13		1	9
Total	14	22	34	14	23	34

Table 22: Planning arrangements against responsibility, day-to-day and implementation

CONCLUSIONS

There are clear conclusions that may be drawn from this survey, even though the sample size is small. The statistics overwhelmingly describe a situation where senior management have abdicated responsibility for business contingency planning to the IT manager. Furthermore, in just too many cases, it is apparent that planning has not been done, or else not tested and revised. The risks that are taken on are very high. Almost routinely there are minor interruptions and disruptions to IT services. Major incidents have the potential to cripple or destroy organisations. While the routine may be dealt with by most IT professionals - with or without a plan - major incidents are not best 'muddled through'.

This investigation had raised a considerable number of research questions. Prime among these are questions concerning the plans or their absence: Do the espoused reasons of low priority and insufficient resources stand up to detailed examination? Why are IT managers given the planning responsibility? A second set of hypotheses concerns the quality and potential effectiveness of the plans. Why is testing so rare and infrequent? Why are standards and legislation ignored? Are the standards themselves adequate? This research program has many issues to face before Australian business disaster recovery planning is at a sufficient standard.

REFERENCES

Brancheau, J. C. and Wetherbe, J.C. (1987) 'Key Issues in Information Systems Management', **MIS Quarterly, 11**, 1, March 1987, 23-45

Brancheau, J.C., Janz, B.D. and Wetherbe, J.C. (1996) 'Key Issues in Information Systems Management: 1994-5 SIM Delphi Results', **MIS Quarterly, 20**, 2, 225-242

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

Dickson, G. W., Leitheiser, R. L., Wetherbe, J. C. and Niechis, M. (1984) 'Key Information System Issues for the 1980s', **MIS Quarterly, 8**, 4, September 1984, 257-266

Earl, M. J. (1989) **Management Strategies for IT**, Prentice Hall, Hemel Hempstead, UK

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

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

Hartog, C. and Herbert, M. (1986) '1985 Opinion Survey of MIS Managers: Key Issues', **MIS Quarterly**, **10**, 4, December 1986, 351-361

IBM (1996) **A Risk too Far**, IBM, London, with Cranfield University, Cranfield, UK

Lederer, A. L. and Mendelow, A. L. (1986) 'Issues in Information Systems Planning', **Information & Management, 11**, 245-254

Musson, D. and Jordan, E. (1997) 'Business and Computer Contingency Planning in Australia,' Macquarie Graduate School of Management Working Paper 97/40.

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

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

Rothstein, P.-J. (1988) 'Up and running' **Datamation,** 15 October, p87

Securicor (1996) 'Data Security Report' **Information Mgmt & Computer Security**, **4**, 2, 14-17
Standards Australia (1996) **Information security management**, AS/NZS 4444:1996, Sydney
Strategic Publishing (1996) **The MIS 4000**, Strategic Publishing Group, Sydney
Survive! (1996) **Survive! Survey of disaster recovery**, Survive!, London

ACKNOWLEDGMENT

The authors wish to thank Data Security Services, a division of Ausdoc, for their sponsorship and support of this project.