IT contingency planning: management roles

Ernest Jordan
Professor of Management, Macquarie Graduate School of Management, Sydney, Australia

Keywords
Contigency planning, Information technology, Strategic management, Australia

Abstract
This paper presents an analysis of selected participants in a survey of Australian organisations' approaches to business and information technology (IT) contingency planning. In particular, it examines the role of management in planning and setting priorities for contingency planning, especially in those organisations that have specified that IT is critical to the business operations. The survey was undertaken because there was a perception that coping with disaster is a much-neglected aspect of management in Australia, and this analysis examines the underlying attitudes. 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. Managers in the IT area are also expected to take the responsibility for contingency planning for the whole business.

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

Information Management & Computer Security
7/5 [1999] 232–238
© MCB University Press
[ISSN 0968-5227]

Introduction

Security and control has long lost its glamour to the MIS manager. In 1987, Brancheau and Wetherbe showed that "security and control" was only ranked 18th in the list of key issues to MIS managers. 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 a more recent (1994-5) survey in the series (Brancheau *et al.*, 1996), security and control has disappeared completely. However the top item in the 1994-5 survey was "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.

This journal and others regularly publish large scale surveys of current practices with respect to IT contingency planning and security (Kearvell-White 1996a, b; Securicor, 1996; Ernst and Young, 1996; NCC 1994, 1996; IBM, 1996; Survive, 1996). One aim of this investigation was to determine whether Australian practice mirrored international standards; a further aim was to explore management attitudes. The research addresses three key areas:

1 the extent of planning;
2 organisational roles and responsibilities; and
3 other risk and security policies.

The overall aims were to find out whether Australian businesses are taking the risks to their businesses and IT seriously; to establish the level of awareness and preparedness; and to plan interventions such as education, workshops and self-assessment schedules. This is examined from the point of view of those organisations that specified that they were highly dependent on IT as it isolates organisations that should be protecting their businesses most thoroughly.

This paper seeks to examine in some detail the role of management in contingency planning and raise specific questions that can be addressed in subsequent research. It does this through consideration of three main aspects: experienced contingencies, plan management and relationship to other risks.

Experiences

There are 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.

Plan management

The simplest, clearest and most widely agreed strategy to deal with contingencies is to have a plan (such as described in Standards Australia, 1996). 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. 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.

Other risks

Information technology is not the only area of risk in keeping an organisation operational. We therefore decided to see whether attitudes to IT risk were mirrored in attitudes to crisis management, document security and business risk. In this region we have recently experienced crises in public utilities that have had profound consequences to some businesses. The monopoly gas supplier in Victoria was, for some two weeks, unable to supply to its millions of

The current issue and full text archive of this journal is available at
http://www.emerald-library.com

domestic, commercial and industrial consumers; in Sydney the water supply was subject to health warnings for many weeks with consequent effects especially for hotels and restaurants. In Auckland, New Zealand, the central business district lost its entire electricity supply for more than two months in 1998. Will these experienced crises change management attitudes or practices? We believe not.

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.

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:

1 it was anticipated that the overall level of preparedness would be high because of mandatory controls; and
2 we expected some reluctance to respond from such organisations.

We further restricted ourselves to Australian organisations with significant computer configurations. This was prompted by the fact that, as the research was to a great extent exploratory, only a sample survey was to be undertaken, and it was necessary to balance the spread of the sample against the depth that could be achieved in a restricted population.

As we believe that overall business contingency planning needs, in our opinion, to be the responsibility of senior executives, we decided to target the CEO of organisations. A letter, designed to be both provocative and informative, aimed to obtain high level commitment within the target organisations. It was addressed to the chief executive (or equivalent) of the organisation, and it asked the recipient to pass on the questionnaire to the IT manager or contingency planning manager in the organisation. The letter also asked the recipient to complete the notification form, giving the name of the person to whom the questionnaire had been passed. The notification form also asked the chief executives whether they would like a copy of the survey report when it was issued. This procedure helped secure a good response rate.

The mailing list was based upon the MIS 4000 database of Australian and New Zealand computer users, ranked by the number of computer screens in the organisation (Strategic Publishing, 1996). Computer screens counted include personal computers, workstations, laptops and dumb terminals. This database lists 4,169 computer users. Nineteen per cent (or 792) of these were in New Zealand, 16.4 per cent (or 684) of these were in the public service and 5.7 per cent (or 238) were IT suppliers. Excluding these gave a total of 2,455 users. Thirty-one other organisations were also excluded; mainly holding companies whose operating companies were also listed. This left a total of 2,424 organisations. A stratified random sample of 283 organisations was selected, representing ten per cent of the larger industry groups and some 20 per cent of the smaller industry groups.

The questionnaire contained questions in the following categories: demographic, experienced contingencies, attitudes to planning, actual planning and backup procedures.

Results

Approximately 25 per cent of the questionnaires were returned in a useable form. Demographic analysis of the non-responses suggested that the respondents were representative of the whole population. Detailed tabulations of the original data are published elsewhere (reference available after refereeing). This paper examines in some detail the management attitudes and practices. In some organisations IT has only a support role but we wish to look at organisations for which some planning is essential. This paper therefore only reports on the responses in 27 organisations where the IT has been assessed by the respondent to be critical. This selection is based on the response to the question: What is the maximum acceptable out-of-service time for your IT services? We report only on those responses that selected the shortest time frame – less than eight hours.

Planning situation

We were concerned to know the frequency with which organisations held plans, both for IT and for the business operations. The question made it clear that a fully documented plan was being referred to. Although answers to subsequent questions made it clear that some organisations had some form of plan, it needs to be documented to meet Australian standards.

Table I shows that only five of 27 organisations had comprehensive plans both for IT and for the business operations. A further three organisations had an IT plan. This is a very low level of compliance and must represent an unacceptable level of risk. It is worth remembering that all 27 organisations have indicated that a disruption of less than eight hours is critical.

A confirmatory question in a different area of the questionnaire asked how long the plans had been held. The responses confirm that only five do have business plans (Table II). Furthermore the existing plans had only been available for short durations. A similar pattern is shown in the IT plans (see Table III), except that there were some plans of longer duration.

If the data in Table III represented organisations for which IT performed only a support role, it would be possible to understand the low level of planning. However, the 27 organisations are only those that have indicated that a disruption of less than eight hours is the maximum tolerable.

The issues that arise immediately are: "Is this just bad management or do these organisations not experience problems?" Let us examine these items.

Table I
Frequency of business and IT contingency planning, affirmative responses: "Does your company have comprehensive plans?"

	Frequency	Percentage
For your complete business operations including IT	5	18.5
For your IT only	3	11.1
For neither business nor IT	19	70.4
Total	27	100.0

Table II
Duration of business contingency plan: "How long have you had your business plans?"

	Frequency	Percentage
Less than 1 year	1	3.7
1-2 years	3	11.1
More than 5 years	1	77.8
No plan	21	3.7
Being developed but not ready	27	100.0

Table III
Duration of IT contingency plan: "How long have you had your IT plans?"

	Frequency	Percentage
Less than 1 year	3	11.1
1-2 years	2	7.4
3-5 years	1	3.7
More than 5 years	2	7.4
No plans	18	66.7
Being developed but not yet ready	1	3.7
Total	27	100.0

Management

Who is responsible for this planning situation? We dealt with this question by contrasting the day-to-day issue of developing plans with the responsibility in an emergency. The person responsible for contingency planning is shown in Table IV.

The IT manager is the person most frequently cited as having responsibility for planning, but nine organisations did not feel it was necessary to have plans or it was not anyone's responsibility. This is an overwhelming situation. Giving the planning responsibility to the IT manager is only reasonable for very few organisations. It is hard to say whether it is worse to make a regular staff member responsible for contingency planning or to have no one responsible. We would argue that the responsibility for ensuring that the organisation has plans should be at a high level, such as the CEO, but that the plans should be written and maintained by the IT and operations managers.

Were an emergency to eventuate, the dogged IT manager becomes the captain at the wheel of the shipwreck. Eight organisations appear not to have decided who will take up this role (Table V). Only six organisations have what we regard as appropriate answers, that the responsibility in an emergency becomes one for a board member.

The significant question is, of course, whether such ill-prepared organisations would be able to deal with an emergency. Table VI shows that the level of confidence has an unreasonable correspondence to the level of preparedness. Recall that only five organisations have comprehensive plans, yet ten organisations express a significant level of confidence. The nine respondents who lack any confidence in their organisation's ability to survive are not just prophets of doom.

Table IV
Responsibility for creating contingency plans: "Who is responsible on a day-to-day basis for your plans?"

	Frequency	Percentage
IT manager	12	44.4
Line manager	4	14.8
Staff members	2	7.4
No plans	9	33.3
Total	27	100.0

Table V
Responsibility for implementation of contingency plan: "Who ensures implementation of your plans in an emergency?"

	Frequency	Percentage
MD/chief executive	3	11.1
Main board member	3	11.1
IT manager	10	37.0
Line manager	1	3.7
Staff member	2	7.4
No plans	8	29.6
Total	27	100.0

Table VI
Confidence in effectiveness of contingency plans: "Are you confident that your plans will ensure the survival of your business?"

	Frequency	Percentage
No answer	1	3.7
Yes, completely confident	3	11.1
Yes, I believe they will	7	25.9
They probably will	7	25.9
I am sure that they will	9	33.3
Total	27	100.0

Experiences

Many questions in the questionnaire dealt with frequency and reliability of backup as well as testing of plans, a serious matter in its own right (Maslen, 1996). To illustrate that some level of preparedness is necessary we reproduce only the data concerning interruptions that were experienced in the previous year. The precise counts that were delivered in these responses gave us confidence that the answers were accurate.

Table VII shows that ten of the 27 organisations had experienced short interruptions of less than one hour, while Table VIII looks at longer interruptions. Again ten organisations had experienced delays of up to four hours. So we are in the situation where ten organisations have experienced delays that can be compared with the self-defined maximum acceptable (of eight hours) yet only five have comprehensive plans.

Table VII
Number of organisations experiencing short interruptions: "Number of interruptions of less than one hour"

	Frequency	Percentage
1	2	7.4
2	2	7.4
3	2	7.4
4	1	3.7
7	1	3.7
10	2	7.4
Nil	17	63.0
Total	27	100.0

Table VIII
Number of organisations experiencing longer interruptions: "Number of interruptions between one and four hours"

	Frequency	Percentage
1	1	3.7
2	2	7.4
3	2	7.4
4	2	7.4
5	1	3.7
10	1	3.7
24	1	3.7
Nil	17	63.0
Total	27	100.0

Other risks in the organisation

For many organisations IT is critical and it must be safeguarded but there are other risks that are faced (FEMA, 1996; Hardy, 1992). Crises such as loss of utilities, closure of roads, bankruptcy of a major customer, floods, loss of original physical documents, are all matters that need to be considered (Pearson *et al.*, 1997). The lack of planning demonstrated in the IT domain is mirrored elsewhere in the organisation (see Tables IX-XII). A case study of a recent fire in a major organisation (unpublished) has shown a complete absence of planning for any contingencies such as loss of key personnel, loss of office space, loss of telephone systems, physical security against threats and also its irreplaceable paper records.

A business recovery policy would be brought into action in the event of extortion, serious negative publicity or an event that caused business activity to cease, without damage or direct impact on the means of production or other operational activity. It could even be the loss of a major customer or protected business environment. The level of preparedness in this area is higher (Table IX) but still not at a level that gives any assurance. Future investigations will attempt to determine whether this higher level of preparedness is through retention of public

Table IX
Ownership of business recovery policies: "Do you have a formal policy for business recovery?"

	Frequency	Percentage
No	16	59.3
Yes	11	40.7
Total	27	100.0

relations and legal consultants, who are able to step in in such circumstances. Alternatively it could be that senior executives are themselves prepared for such activity.

A crisis management policy can only deal with management responsibility for such events, as the events are, by definition, not anticipated. Each crisis needs to be dealt with on an individual basis and management actions need to be taken to suit the situation at hand. Crises are not predictable nor may specific planning be undertaken for them. Thus a crisis management plan should be somewhat shorter than an IT or business contingency plan, where specific contingencies need to be addressed in detail. Nevertheless, we still find that the majority of the organisations do not have these plans (see Table X).

Risk management represents a formal scanning of the organisation's environment, seeking to determine an exhaustive list of risks and threats that may face the organisation. Internal or operational risks also need to be tabulated. For each risk a different form of response may be necessary. Again it is often a managerial issue – deciding under what circumstances events must be escalated to more senior management. More importantly it is a guard against the "boiled frog" syndrome, where situations gradually deteriorate without any specific critical point being identified. Each manager would have a schedule of risk items in their domain. These need to be regularly scanned and assessed. If they reach a specific level, a response is required. Table XI shows that risk management, like business recovery, appears to be treated a little more seriously. Future research will also examine the factors at work here.

Table X
Ownership of crisis management policies: "Do you have a formal policy for crisis management?"

	Frequency	Percentage
No	18	66.7
Yes	9	33.3
Total	27	100.0

Table XI
Ownership of risk management policies: "Do you have a formal policy for risk management?"

	Frequency	Percentage
No	16	59.3
Yes	11	40.7
Total	27	100.0

Protection of vital records is the only area where a clear majority of the organisations are taking preventative action and devising appropriate plans, as shown in Table XII. Why should this be the case? It could be that our term "vital" allowed organisations to cover themselves more readily. That is, a relatively unprepared organisation may only regard a very restricted set of documents to be "vital records", where a more conscientious organisation may take a broader, all-encompassing view. Using this generous interpretation, there are still one-third of organisations that do not even safeguard those documents that they themselves regard to be vital.

Viewed positively, some two thirds of organisations are taking a more careful and considered approach to maintaining their records than they are towards business operations, IT contingency, risks or crises. It may also be that "records" are generally tangible and identifiable, and thus may more readily be the focus of a security policy. This also represents an area for further investigation.

Future actions

Are you going to do any planning? Is this something that your organisation was aware of? Before we attempt to answer these questions, it is useful to investigate the reasoning behind the absence of plans. As shown in Table XIII, below, contingency planning is certainly of a low priority; it is also seen to

Table XII
Ownership of vital record policies: "Do you have a formal policy for vital records?"

	Frequency	Percentage
No	9	33.3
Yes	18	66.7
Total	27	100.0

Table XIII
Reasons for absence of IT contingency plan: "What is the main reason for not having an IT plan?"

	Frequency	Percentage
Considered necessary but low priority	11	40.7
Not considered	1	3.7
Insufficient resources	5	18.5
Don't know	1	3.7
Being developed but not ready	1	3.7
Missing (have plans)	8	29.6
Total	27	100.0

demand resources. Many IT vendors offer IT contingency planning services that are based on a percentage of the value of the installed hardware base. While this may be an unreasonable charging mechanism, it represents a significant amount of funds for any organisation. Additional resources involved include the personnel and the time involved in devising and testing plans. If the cost for these plans needs to be taken from the IT manager's budget – and that is seen as an overhead – then the situation will persist.

Table XIV shows that the reasons for not having business contingency plans are very similar to those for the absence of IT contingency plans, with lack of resources and low priority again dominating. While it may be reasonable in some organisations for traditional attitudes towards IT to persist, that it is seen as a cost, an overhead, it is unreasonable for the business to be seen in this way. The results show that protecting the business is a low priority. One view is that a line needs to be drawn between those contingencies or difficulties that we guard against, and those that we will deal with as and when they happen. For many individuals and businesses, house and property insurance against physical loss and third party liability will be on one side of the line, with contingent impacts on the other side of the line. You insure your building, but not the loss of work or other impacts of building destruction – yet real disasters often reveal contingent costs that rival or exceed the costs of physical replacement.

As a final matter, the respondents were asked their intention towards business contingency planning in the future. There is some sense of urgency for 40 per cent of the respondents (Table XV), but many remain unlikely to develop plans. It is quite possible that the sense of urgency diminished dramatically as soon as the survey document was put in its envelope. Only an optimist would expect that a case-by-case follow up of the respondents would reveal some adherence to these intentions.

Table XIV
Reasons for absence of business contingency plan: "What is the main reason for not having a business plan?"

	Frequency	Percentage
No answer	2	7.4
Considered necessary but low priority	7	25.9
Not considered necessary	1	3.7
Not considered	2	7.4
Insufficient resources	5	18.5
Don't know	4	14.8
Being developed but not ready	1	3.7
Missing (have plans)	5	18.56
Total	27	100.0

Table XV
Future business contingency planning schedule: "When do you intend to produce business contigency plans?"

	Frequency	Percentage
No answer	5	18.5
In the next year	8	29.6
In 1-2 years	3	11.1
In 2 years +	1	3.7
Do not intend to produce them	4	14.8
Plan exists but is not documented	1	3.7
Missing (have plans)	5	18.5
Total	27	100.0

On the other hand, IT contingency plans were anticipated to be developed in the next year by more than half of the respondents, two-thirds of those without current plans (Table XVI). This is likely to have been a year 2000 (Y2K) development, with contingency planning seen as one part of the necessary Y2K response. Note that it appears under IT – there is no such phenomenon under the heading of business contingency planning where it necessarily should appear.

The issue of Y2K preparedness was specifically omitted from the survey as there has been inordinate publicity on the matter, and legal liabilities and responsibilities could cloud the responses. Telephone follow-up of some non-respondents indicated that they had been excessively surveyed on Y2K and were reluctant to get into a situation where potential liabilities were made explicit.

Discussion

The dominant reasons given by those without plans are: insufficient resources and low priority. These appear to be a clear

Table XVI
Future IT contingency planning schedule: "When do you intend to produce IT contigency plans?"

	Frequency	Percentage
In the next year	14	51.9
In 1-2 years	3	11.1
In 2 years +	1	3.7
Do not intend to produce them	1	3.7
Missing	8	29.6
Total	27	100.0

indication of what managers think. In spite of IT being critical to the organisations analysed, it is still seen as a cost, an extra burden on doing business, rather than a necessity or driving force. Adding security to the IT cost, simply increases the costs. It appears that the benefits of contingency planning are seen to be delivered only in an emergency. What benefits are delivered today by a disaster recovery plan? Is it just the warm feeling of security? Is it a better understanding of the business and its critical components? Further in-depth research of organisations that have implemented plans should aim to identify these benefits.

While IT has often been treated as a corporate orphan, there is no reason that operational managers and board members should ignore the continuity of the whole business. Yet this appears to be the case. Attitudes to crises, risk, business recovery and vital records are, to put it mildly, complacent. Perhaps this is the Australian laconic "she'll be right, mate" expressed as a corporate security policy. Managers expect to muddle through, crash through or crash. "We will deal with it when it happens!" These policies and attitudes are not proclaimed in Annual Reports to shareholders, however. The Australian Stock Exchange (ASX) requirement for organisations to report on their Y2K preparedness is perhaps a step in this direction.

Conclusion

This paper has analysed in some detail the attitudes of managers of 27 organisations, where IT is critical to the business. Only five organisations have comprehensive continuity plans for IT and the business, with three others having IT plans. This very low level of preparedness is mirrored in their attitudes towards other corporate risk and security policies.

Responsibility for such matters is generally at too low a level in the organisation and this does not appear to be likely to change in the near future.

Further work is required to determine the advantages and benefits that are perceived to be delivered at the time of contingency planning, as well as the driving factors behind the higher level of priority to business records.

References and further reading

Brancheau, J.C. and Wetherbe, J.C. (1987), "Key issues in information systems management", *MIS Quarterly*, Vol. 11 No. 1, March, pp. 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*, Vol. 20 No. 2, pp. 225-42.

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

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

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

Hardy, K. (1992), "Contingency planning", *Business Quarterly*, Vol. 56 No. 4, Spring, pp. 26-8.

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

Kearvell-White, B. (1996a), "KPMG's UK computer security review 1994", *Information Management and Computer Security*, Vol. 4 No. 2, pp. 42-51.

Kearvell-White, B. (1996b), "National (UK) computer security survey 1996", *Information Management and Computer Security*, Vol. 4 No. 3, pp. 3-17.

Maslen, C. (1996), "Testing the plan is more important than the plan itself", *Information Management and Computer Security*, Vol. 4 No. 3, pp. 26-9.

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

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

Pearson, C.M., Clair, J.A., Misra, S.K. and Mitroff, I.I. (1997), "Managing the unthinkable", *Organizational Dynamics*, Vol. 26 No. 2, pp. 51-64.

Securicor (1996), "Data security report" *Information Management and Computer Security*, Vol. 4, No. 2, pp. 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.