Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2004 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2004

Allocating Redundancy to Critical Information Technology Functions for Disaster Recovery

Benjamin Shao
Arizona State University

Allocating Redundancy to Critical Information Technology Functions for Disaster Recovery

Benjamin B. M. Shao
W. P. Carey School of Business
Arizona State University
Ben.Shao@asu.edu

ABSTRACT

In the present network economy, businesses are becoming increasingly reliant on information technology (IT) to perform their operations and exchange information with business partners. This heavy dependence on IT, however, poses a potential threat for an organization. When natural or man-made disasters strike and cause malfunction to its computing and communicating systems, it would be vulnerable to business discontinuity. Severe consequences resulting from such IT breakdown may include the loss of sales, damages to reputation and consumer confidence, penalty incurred by failure to fulfill the orders, and so on. As a result, the issue of how to strengthen IT capabilities so that a company can prevent or quickly recover from disasters becomes a serious concern. In this paper, we present a discrete optimization model to allocate redundancy to critical IT assets for disaster recovery planning. The objective is to maximize the overall survivability of an organization's critical IT functions by selecting their appropriate redundancy levels while still satisfying a budgetary resource constraint. A solution procedure based on probabilistic dynamic programming is proposed to solve the formulated problem, and two concrete examples are discussed to illustrate its usage and effectiveness.

Keywords

IT disaster recovery, redundancy allocation, discrete optimization, decision-making, dynamic programming.

INTRODUCTION

Modern organizations have become increasingly dependent on information technology (IT) to facilitate their businesses. Large-scale databases handled by high-speed computers retrieve, analyze and synthesize data collected from different sources. Communication networks like the Internet exchange, share, and transmit information in real time between suppliers, vendors and buyers in an industry value chain to carry out business transactions. Computer-aided design technologies help the product development team capture more customer requirements and develop better products to meet their specific needs. These few examples demonstrate that IT is being harnessed as a key enabler for an organization's operations in the present network economy. The prowess of advanced IT represents numerous business benefits for a firm, including enhanced productivity, increased flexibility, better quality, and reduced costs. Utilized properly and creatively, IT can provide competitive advantages for a firm to improve its competitive position by removing competition barriers based on time and distance (Iyer and Sarkis, 1998).

This increased reliance on IT, however, poses a potential threat for an organization. When the occurrence of catastrophic events or disasters affects its IT operations and causes their failures, the organization may suffer from the interruption of their supported business functions. Severe consequences resulting from such IT breakdown may include the loss of sales, damages to reputation and consumer confidence, penalty incurred by failure to fulfill the orders, and so on. As a consequence, the issue of how to strengthen IT capabilities so that a company can prevent or quickly recover from disasters becomes a serious concern. Clearly, an organization depending on IT to support its business processes and functions needs effective IT security measures to ensure business continuity in the event of disaster strikes (Lewis, Watson, and Pickren, 2003).

Many kinds of potential disasters may immobilize an organization's IT capabilities (Chengalur-Smith, Belardo, and Pazer, 1999). Natural disasters like flood, earthquake, hurricane, tornado, blizzard, etc. are frequently encountered. Disasters can also be man-made, either intentional or unintentional, such as terrorist attacks, computer hackers, virus attacks, union strikes, unreliable hardware, and faulty software. Management has to be aware of the risks to which their business operations are exposed and recognize the threats and events that are likely to occur in the environment in which their firm is operated (Jenkins, 2000). Further, firms in the network economy no longer suffer alone from disasters. When a disaster occurs, business partners, both upstream and downstream in the industry value chain, may too suffer from the concomitant

consequences. In other words, the effects caused by a disaster can migrate to other entities over either the virtual or physical network. A thorough decision analysis aids in identifying, evaluating, and strengthening critical IT functions that must be maintained in case of a disaster (Tamura, Yamamoto, Tomiyama, and Hatono, 2000).

A disaster recovery plan is defined as a system for internal control and security that focuses on quick restoration for critical organizational processes when there are operational failures due to natural or man-made disaster (Bryson, Millar, Joseph, and Mobolurin, 2002). The objective of an IT disaster recovery plan is to ensure that an organization's computing and communication systems operate smoothly and uninterruptedly during and after the occurrence of a disaster. Once equipped with an effective IT disaster recovery plan, an organization is better prepared and can minimize potential loss by identifying, prioritizing and safeguarding valuable IT assets that need protection. On the contrary, an unprepared business without an IT disaster recovery plan in place is likely to suffer from the loss of information and the inability to continue its operations due to disaster.

Despite the unequivocal importance of IT disaster recovery planning, little research has been done so far on the formal modeling of its decision-making process. It has been suggested that many of the issues encountered in disaster recovery planning can benefit from the application of quantitative decision-making techniques (Bryson, Millar, Joseph, and Mobolurin, 2002). In this paper, a discrete optimization model is proposed to assist IT managers in allocating appropriate redundancy level for valuable IT assets so that the overall risks against potential disasters can be reduced. Our model takes into account the criticality and costs of various IT assets as well as the resource limitation subject to budget availability.

The remainder of this paper is organized as follows. Section 2 discusses the concept of using redundancy as a protective means to prepare for IT disasters. The mathematical optimization model for redundancy allocation is presented in Section 3. A solution procedure based on probabilistic dynamic programming is proposed in Section 4, along with the illustration of two specific examples. Finally, the conclusion and some topics suggested for future research are given in Section 5.

REDUNDANCY FOR IT DISASTER RECOVERY

The use of redundancy in preparation for disasters is of potential advantage because it can simultaneously address two aspects of disaster preparation – proactive prevention and reactive recovery. Before a disaster occurs, redundant components can mitigate the potential risks by working as backup facilities and thus preventing the disastrous consequences in advance (Grabowski, Merrick, Harrald, Mazzuchi, and van Dorp, 2000). After the occurrence of a disaster, organizations can quickly restore business functions and processes back to normal by substituting redundant components for the primary but disabled parts while they are being repaired and restored.

So far the practice of IT disaster recovery planning has been focused on data recovery and program resumption. Most organizations nowadays already have daily backup procedures for data and programs, but these procedures alone may not be sufficient for restoring business functions and processes back to normal promptly enough to ensure business continuity (Iyer and Sarkis, 1998). While these backup and recovery procedures are necessary for resuming the information flow, they are essentially reactive and passive in nature, limited in their functionality. There are many other vital IT functions that also need be enacted. Such reaction-based measures thus can be enhanced by incorporating redundancy for every critical IT asset.

In an organization, the same IT function can be implemented by a number of IT assets. For example, the data backup procedure can be performed using inexpensive magnetic tapes, moderately expensive CD-RW, expensive redundant array of independent disks (RAID), or a combination of these technologies together for redundancy. The IT assets considered here are comprehensive and vary in scope. They can include tangible computing hardware, communication links, IT personnel, and other infrastructure that serve as the means by which data are transmitted, processed, or presented for certain IT functions. Alternatively, they can be intangible assets like databases containing sensitive customer information or software programs developed for data manipulation. In terms of scope, these IT assets can be as small as redundant modules for fault-tolerant software, or be as large as a backup hot site that has replicated almost everything for the whole IT department.

Clearly, IT assets differ in their potential risks and costs. As such, redundancy at different levels also has different cost and benefit implications. A redundant module in fault-tolerant software would likely cost only a little to develop but the risk mitigated by its presence is probably small as well. On the other hand, a full-scale duplicated hot site requires a large investment but can provide a much better protection against a disaster; thus, it may be a viable option for large size companies only. The objective is thus to select among these competing alternatives for redundancy level and reap the best returns subject to resource limitations. A quantitative analytical model can provide the guidelines for allocating the optimal redundancy level to critical IT functions that need the most protection in a cost-conscious and rational way.

While the technique of integer programming has recently been applied to the selection of disaster scenarios (Jenkin, 2000), most studies have either focused on the area of risk analysis (Tamura, Yamamoto, Tomiyama, and Hatono, 2000) or been

reactive in nature by primarily dealing with the post-disaster operational activities (Pidd, deSilva, and Eglese, 1996). In answer to the call for more rigorous quantitative analyses of the pre-disaster IT recovery planning (Bryson, Millar, Joseph, and Mobolurin, 2002), we develop a discrete optimization model to help ensure that IT disaster recovery plans function as expected when put into work.

REDUNDANCY ALLOCATION MODEL

Suppose a firm is planning for disaster recovery by considering incorporating redundancy level for its IT functions, and the budget is limited. Several possible disasters have been identified with the potential to cause business discontinuity by affecting the supporting IT functions. The question is how to allocate redundancy to these IT functions such that the overall survivability of these IT functions against disasters is maximized and the cost remains under budget. Below are the parameter notations and their definitions used in the model.

D: number of potential disasters + 1 (the last one for no disaster occurring);

p_d: probability of disaster d occurring, $p_d \in (0, 1)$ and $\sum_{d=1}^{D} p_d = 1$;

M: number of IT functions the organization needs to perform;

w_m: importance weight (or frequency of usage) of IT function m, $w_m \in (0, 1)$ and $\sum_{m=1}^{M} w_m = 1$;

n_m: number of solutions (assets) available for IT function m to select from;

X_{mi}: 1 if solution i (= 1, …, n_m) is selected for IT function m, or 0 otherwise;

C_{mi}: cost of selecting solution i for IT function m;

S_{mid}: survivability of solution i for IT function m against disaster d;

e_{mid}: failure probability of solution i for IT function m against disaster d, $e_{mid} = 1 - S_{mid}$;

B: available budget.

The following model is formulated to maximize the overall survivability of the M independent IT functions:

$$\text{(RAP)} \quad \max S^* = \sum_{d=1}^{D} p_d \sum_{m=1}^{M} w_m \left[1 - \prod_{i=1}^{n_m} e_{mid}^{\,X_{mi}} \right]$$

subject to

$$\sum_{i=1}^{n_m} X_{mi} \geq 1, m = 1, \ldots, M \tag{1}$$

$$\sum_{m=1}^{M} \sum_{i=1}^{n_m} C_{mi} X_{mi} \leq B \tag{2}$$

$$X_{mi} = 0 \text{ or } 1, \quad \text{for } m = 1,..., M \text{ and } i = 1,..., n_m \tag{3}$$

It is assumed the occurring probability p_d of a certain disaster d is known or can be estimated. The parameter D is equal to the number of potential disasters plus one. The last additional one corresponds to the case when no disaster actually occurs (i.e., $p_D = 1 - \sum_{d=1}^{D-1} p_d$). Moreover, the IT functions are regarded as separate and independent. The criticality of a certain IT function is measured by its frequency of usage. The rationale is that the more frequently an IT function is used to support business operations, the more importance it carries for the organization. There exists a pool of n_m candidate IT assets (solutions) to select from for IT function m. When a certain IT asset i is selected for IT function m, its corresponding decision variable X_{mi} is set to 1, or 0 otherwise.

In (RAP), the objective function tries to maximize the overall survivability of all IT functions against all potential disasters. It reflects the fact that an IT function *m* fails against a certain disaster *d* only when all of its selected solutions fail at the same time. In other words, as long as one of the selected solutions survives the disaster, IT function *m* would still be operational, thus $\left[1-\prod_{i=1}^{n_m} e_{mid}{}^{X_{mi}}\right]$. Constraint (1) ensures that at least one IT solution be selected and allocated to each IT function. This, however, implies that it is possible for some IT functions to have only one solution allocated without redundancy. In case we must have at least some standby solution for every IT function, we need to only change the constant on the right hand side of constraint (1) from 1 to 2. Constraint (2) guarantees that the total costs of redundancy allocation not exceed the budget limitation. To provide a systematic view on the problem, Figure 1 illustrates the scenario that (RAP) attempts to resolve.

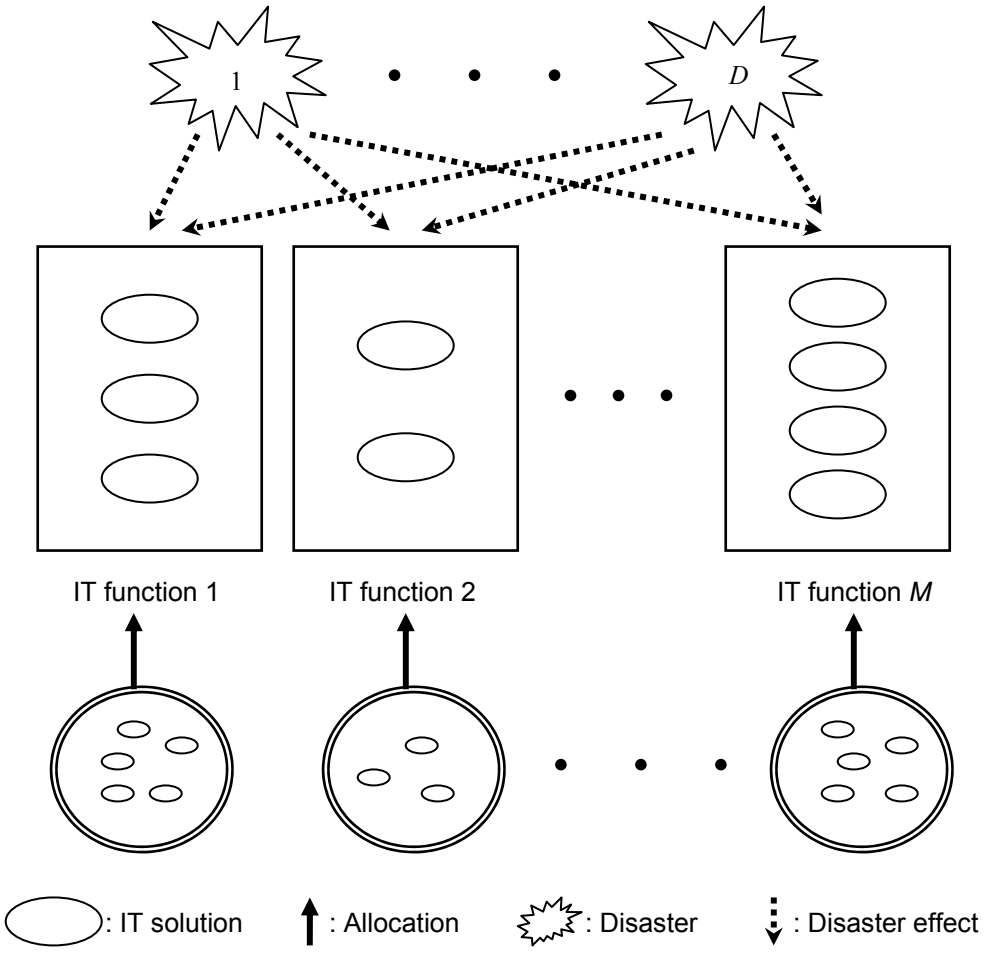

Figure 1. Redundancy Allocation Scenario for Disaster Recovery Planning

SOLUTION PROCEDURE AND EXAMPLES

The proposed model of (RAP) is a 0-1 integer programming problem with a nonlinear objective function. For small problem instances, total enumeration or mathematical software packages can be used to solve (RAP). However, for relatively large problems, such approaches are likely impractical. Further, owing to the non-linearity of the objective function, Lagrangian relaxation cannot be employed to help tackle this discrete optimization problem. As such, a partial enumeration solution procedure based on probabilistic dynamic programming (Winston, 1987) is presented to help the solution of (RAP). We first can reformulate (RAP) as a minimization problem by rewriting the objective function as follows:

$$S^* = \sum_{d=1}^{D} p_d \sum_{m=1}^{M} w_m \left[1 - \prod_{i=1}^{n_m} e_{mid}^{\ X_{mi}} \right] = \sum_{d=1}^{D} p_d \sum_{m=1}^{M} w_m - \sum_{d=1}^{D} p_d \sum_{m=1}^{M} w_m \prod_{i=1}^{n_m} e_{mid}^{\ X_{mi}}$$

$$= \sum_{d=1}^{D} p_d - \sum_{d=1}^{D} p_d \sum_{m=1}^{M} w_m \prod_{i=1}^{n_m} e_{mid}^{\ X_{mi}} = 1 - \sum_{d=1}^{D} p_d \sum_{m=1}^{M} w_m \prod_{i=1}^{n_m} e_{mid}^{\ X_{mi}}$$

To maximize S^* is equivalent to minimizing $F^* = \sum_{d=1}^{D} p_d \sum_{m=1}^{M} w_m \prod_{i=1}^{n_m} e_{mid}^{\ X_{mi}}$, which is the sum of failure probabilities of any IT function due to any disaster. Next, we define a state of system T as the budget available, and stage m to represent IT function m for $m = 1, \ldots, M$. Let $F_m(T)$ be the failure rate of the system composed of IT functions $m, m+1, \ldots, M$, given that T is the remaining budget for IT functions $1, \ldots, m-1$. The recursive formula for $F_m(T)$ when $m < M$ is:

$$F_m(T) = \min\left(w_m \sum_{d=1}^{D} p_d \prod_{i=1}^{n_m} e_{mid}^{\ X_{mi}} + F_{m+1}(B - \sum_{i=1}^{n_m} C_{mi} X_{mi}) \right) \tag{4}$$

where the variables X_{mi} are restricted to those that satisfy

$$\sum_{i=1}^{n_m} X_{mi} \geq 1 \quad \text{and} \quad \sum_{i=1}^{n_m} C_{mi} X_{mi} \leq T$$

For stage (IT function) m, state (budget) T cannot exceed the total available budget B minus the minimum costs to be allocated for the remaining stages $1, \ldots, m-1$, and it must be at least equal to the cost of the least expensive solution in the current stage to guarantee at least one solution for IT function m. Thus, $F_m(T)$ should be evaluated for all T values in the range:

$$T = \left(\min_{i=1,\ldots,n_m} \{C_{mi}\}, \ldots, B - \sum_{r=1}^{m-1} \min_{i=1,\ldots,n_r} \{C_{ri}\} \right) \tag{5}$$

For states not in the specified range, $F_m(T)$ can be defined as 1 so it would not become the minimum chosen by Eq. (4) for stages $1, \ldots, m-1$.

The solution procedure is based on probabilistic dynamic programming because, unlike deterministic dynamic programming, $F_m(T)$ of Eq. (4) deals with the uncertainty of disaster occurring and involves the calculation of *expected* failure rate of IT function m based on the remaining budget T. The solution procedure solves (RAP) by working backwards with the initial stage $m = M$ and

$$F_M(T) = \min_{X_{Mi}} \left(w_M \sum_{d=1}^{D} p_d \prod_{i=1}^{n_M} e_{Mid}^{\ X_{Mi}} \right) \tag{6}$$

where again the variables X_{Mi} satisfy

$$\sum_{i=1}^{n_M} X_{Mi} \geq 1 \quad \text{and} \quad \sum_{i=1}^{n_M} C_{Mi} X_{Mi} \leq T$$

Finally, the optimal objective function value F^* is obtained as $F_1(B)$ and represents the minimum overall failure rate of the whole system composed of M independent IT functions with a budget of B. That is, the original maximum overall survivability S^* of (RAP) is equal to $1 - F_1(B)$.

Example 1

To demonstrate the effectiveness of the proposed model and solution procedure, we consider a hypothetical example in which a company performs two IT functions ($M = 2$) for its business operations. IT function 1 is used 30% of the time ($w_1 = 0.30$) and IT function 2 is used 70% of the time ($w_2 = 0.70$). The company is susceptible to a flooding disaster that occurs with a likelihood of 0.05 ($p_1 = 0.05$ and $p_2 = 0.95$ for no disaster). The company is now considering incorporating redundancy for the two IT functions with a budget $B = 14$.

For IT function 1, four solutions are available ($n_1 = 4$), with associated costs of $C_{11} = 8$, $C_{12} = 3$, $C_{13} = 7$, and $C_{14} = 5$. Their survival rates against the flooding are $S_{111} = 0.10$, $S_{121} = 0.05$, $S_{131} = 0.08$, and $S_{141} = 0.12$ (i.e., $e_{111} = 0.90$, $e_{121} = 0.95$, $e_{131} = 0.92$, and $e_{141} = 0.88$). Their reliabilities when no disaster occurs are $S_{112} = 0.95$, $S_{122} = 0.88$, $S_{132} = 0.92$, and $S_{142} = 0.85$ (i.e., $e_{112} = 0.05$, $e_{122} = 0.12$, $e_{132} = 0.08$, and $e_{142} = 0.15$). For IT function 2, three solutions are available ($n_2 = 3$), with associated costs of $C_{21} = 4$, $C_{22} = 6$, and $C_{23} = 3$. Their survival rates against the flooding are $S_{211} = 0.06$, $S_{221} = 0.10$, and $S_{231} = 0.20$ (i.e., $e_{211} = 0.94$, $e_{221} = 0.90$, and $e_{231} = 0.80$). Their reliabilities when no disaster occurs are $S_{212} = 0.92$, $S_{222} = 0.78$, and $S_{232} = 0.84$ (i.e., $e_{212} = 0.08$, $e_{222} = 0.22$, and $e_{232} = 0.16$). The original maximization problem for this example is formulated:

$$\begin{aligned}\max S^* = {} & 0.05\left[0.30\left(1-0.90^{X_{11}}0.95^{X_{12}}0.92^{X_{13}}0.88^{X_{14}}\right)+0.70\left(1-0.94^{X_{21}}0.90^{X_{22}}0.80^{X_{23}}\right)\right] \\ & +0.95\left[0.30\left(1-0.05^{X_{11}}0.12^{X_{12}}0.08^{X_{13}}0.15^{X_{14}}\right)+0.70\left(1-0.08^{X_{21}}0.22^{X_{22}}0.16^{X_{23}}\right)\right]\end{aligned}$$

subject to

$$\begin{aligned}& X_{11}+X_{12}+X_{13}+X_{14}\geq 1 \\ & X_{21}+X_{22}+X_{23}\geq 1 \\ & 8X_{11}+3X_{12}+7X_{13}+5X_{14}+4X_{21}+6X_{22}+3X_{23}\leq 14 \\ & X_{mi}=0 \text{ or } 1, \quad \text{for all } m, i\end{aligned}$$

To apply the solution procedure to this problem instance, we start with stage $m = 2$. Since the least expensive solution for IT function 2 has cost $C_{23} = 3$ and the least expensive solution for the only remaining IT function 1 also has cost $C_{12} = 3$, the valid range for T is $3 \leq T \leq 11$ (= 14 – 3). Eq. (6) then calculates $F_2(T)$ for $T = 3, \ldots, 11$. For instance, $F_2(7)$ is calculated as:

$$F_2(7) = \min\left\{(0.70)[\,(0.05)(0.94)^{X_{21}}(0.90)^{X_{22}}(0.80)^{X_{23}}+(0.95)(0.08)^{X_{21}}(0.22)^{X_{22}}(0.16)^{X_{23}}\,]\right\}$$

where the variables X_{2i} satisfy $X_{21} + X_{22} + X_{23} \geq 1$ and $4X_{21} + 6X_{22} + 3X_{23} \leq 7$. There are four sets of X_{2i} qualified for $F_2(7)$, and they are $(X_{21}, X_{22}, X_{23}) = (0, 0, 1)$, $(0, 1, 0)$, $(1, 0, 0)$, and $(1, 0, 1)$. The minimum $F_2(7) = 0.0348$ is found associated with $(X_{21}, X_{22}, X_{23}) = (1, 0, 1)$. The complete results for $F_2(T)$ are shown in Table 1.

T	Solution	$F_2(T)$
3	$X_{21} = 0, X_{22} = 0, X_{23} = 1$	0.1344
4	$X_{21} = 1, X_{22} = 0, X_{23} = 0$	0.0861
5	$X_{21} = 1, X_{22} = 0, X_{23} = 0$	0.0861
6	$X_{21} = 1, X_{22} = 0, X_{23} = 0$	0.0861
7	$X_{21} = 1, X_{22} = 0, X_{23} = 1$	0.0348
8	$X_{21} = 1, X_{22} = 0, X_{23} = 1$	0.0348
9	$X_{21} = 1, X_{22} = 0, X_{23} = 1$	0.0348
10	$X_{21} = 1, X_{22} = 0, X_{23} = 1$	0.0348
11	$X_{21} = 1, X_{22} = 0, X_{23} = 1$	0.0348

Table 1. State T, Solution, and $F_2(T)$ for Stage 2 with $B = 14$

Next, we proceed to find the optimal solution $F_1(14)$ in the next stage $m = 1$:

$$F_1(14) = \min \{ (0.30)[(0.05)(0.90)^{X_{11}} (0.95)^{X_{12}} (0.92)^{X_{13}} (0.88)^{X_{14}} + (0.95)(0.05)^{X_{11}} (0.12)^{X_{12}} (0.08)^{X_{13}} (0.15)^{X_{14}}] + F_2(14 - \sum_{i=1}^{4} C_{1i} X_{1i})\}$$

where the variables X_{1i} satisfy $X_{11} + X_{12} + X_{13} + X_{14} \geq 1$ and $8X_{11} + 3X_{12} + 7X_{13} + 5X_{14} \leq 14$. There are seven sets of X_{1i} qualified for $F_1(14)$, and they are $(X_{11}, X_{12}, X_{13}, X_{14}) = (1, 0, 0, 0), (0, 1, 0, 0), (0, 0, 1, 0), (0, 0, 0, 1), (1, 1, 0, 0), (0, 1, 1, 0)$, and $(0, 1, 0, 1)$. The minimum $F_1(14)$ is found associated with $(X_{11}, X_{12}, X_{13}, X_{14}) = (0, 0, 1, 0)$ with $F^* = F_1(14) = 0.0714$ using $F_2(7) = 0.0348$. Therefore, the maximum overall survivability S^* against flooding is $1 - F^* = 1 - 0.0714 = 0.9286$ by selecting solution 3 for IT function 1 ($X_{13} = 1$) as well as solutions 1 and 3 for IT function 2 ($X_{21} = X_{23} = 1$).

Example 2

Let us examine the effect of having more budgetary resources for redundancy allocation. Suppose all the data are the same as in Example 1. The only exception is that the company now has a greater budget $B = 16$. Starting with stage $m = 2$, the valid range for T becomes $3 \leq T \leq 13$ $(= 16 - 3)$. The values of $F_2(T)$ for $T = 3, \ldots, 11$ are the same as in Table 1. We thus only need to compute $F_2(T)$ for $T = 12$ and 13. The results are shown in Table 2.

T	Solution	$F_2(T)$
3, …, 11	Same as in Table 1	–
12	$X_{21} = 1, X_{22} = 0, X_{23} = 1$	0.0348
13	$X_{21} = 1, X_{22} = 1, X_{23} = 1$	0.0256

Table 2. State T, Solution, and $F_2(T)$ for Stage 2 with $B = 16$

We next find the optimal solution $F_1(16)$ in the next stage $m = 1$:

$$F_1(16) = \min \{ (0.30)[(0.05)(0.90)^{X_{11}} (0.95)^{X_{12}} (0.92)^{X_{13}} (0.88)^{X_{14}} + (0.95)(0.05)^{X_{11}} (0.12)^{X_{12}} (0.08)^{X_{13}} (0.15)^{X_{14}}] + F_2(16 - \sum_{i=1}^{4} C_{1i} X_{1i})\}$$

where the variables X_{1i} satisfy $X_{11} + X_{12} + X_{13} + X_{14} \geq 1$ and $8X_{11} + 3X_{12} + 7X_{13} + 5X_{14} \leq 16$. There are nine sets of X_{1i} qualified for $F_1(16)$, and they are $(X_{11}, X_{12}, X_{13}, X_{14}) = (1, 0, 0, 0), (0, 1, 0, 0), (0, 0, 1, 0), (0, 0, 0, 1), (1, 1, 0, 0), (1, 0, 0, 1), (0, 1, 1, 0), (0, 1, 0, 1)$, and $(0, 0, 1, 1)$. The minimum $F_1(16)$ is found associated with $(X_{11}, X_{12}, X_{13}, X_{14}) = (0, 1, 0, 1)$ with $F^* = F_1(16) = 0.0525$ using $F_2(8) = 0.0348$. Thus, the maximum overall survivability S^* against flooding has been increased to $1 - F^* = 1 - 0.0525 = 0.9475$ by selecting solutions 2 and 4 for IT function 1 ($X_{12} = X_{14} = 1$) as well as solutions 1 and 3 for IT function 2 ($X_{21} = X_{23} = 1$). In this arrangement, each IT function now has at least one redundant component for disaster recovery.

MODEL APPLICATIONS IN ORGANIZATIONS

The application of the proposed redundancy allocation model to real-world risk analysis of disasters for modern organizations can be enhanced by many techniques that have been developed and employed by companies and institutions in the insurance industry. For example, the likelihood of potential disasters assumed in the model can be estimated to a certain degree by historical data and sophisticated forecasting tools. In addition, the survivability of IT assets to be selected from the pool for each critical IT function can be further guaranteed by either the contracts with vendors or the warrantee offered for IT assets. While the modeling details may be too complicated for managers to fully comprehend, this should not pose any difficulty for its users. For example, the model can be designed as a decision support system with a user-friendly interface to shield managers from such technical intricacies. Managers thus can perform sensitivity analysis easily on IT disaster recovery planning by using the decision support system that incorporates the proposed redundancy allocation model.

CONCLUSIONS

The continued rapid advance in computer and communication technologies enables their widespread use of supporting business processes and functions. Moreover, extensive changes in business process automation and redesign have been made possible by IT as well. The ability of IT to facilitate communication and information exchange in real time has resulted in numerous benefits for a business operating in the present network economy. With the increased importance of IT for the operations of modern organizations, we can anticipate an even greater IT adoption by more industries for a wide variety of applications in the near future.

However, computer and communication systems that serve as the backbone of today's business functions also represent potential vulnerabilities to disasters. When a disaster strikes and causes disruption to a firm's IT functions and thus their supported operations, the event may easily threaten the survival of a business. Managers must perform a business impact analysis to both evaluate the degree to which their IT operations are susceptible to disasters and measure the potential losses caused by such disasters. Then they must take necessary actions to strengthen these IT functions according to their criticality.

The discrete optimization model proposed in the paper can fulfill the need for a structured decision analysis of IT disaster recovery planning. The model attempts to maximize the overall survivability of IT functions against potential disasters by allocating appropriate redundancy levels while taking into account the tradeoff between survival rates and costs of IT solutions selected. The feasible use of mathematical optimization is demonstrated as an effective decision support tool for better resource allocation of redundancy to cope with disaster recovery. The main purpose is to ensure IT capabilities are uninterrupted and their supported business processes operate continuously by using redundant solutions as backup means to weather potential disasters.

It is noted that the proposed model is a generalization of the reliability optimization models for software and hardware (Ashrafi and Berman, 1992). When no disaster is considered possible (i.e., $D = 1$ in our model), (RAP) is reduced to a reliability problem dealing with fault tolerance (Kuo and Prasad, 2000). In other words, the model proposed in the paper is able to handle such special cases of software and hardware reliability as well. In addition, (RAP) is related to the general discrete resource allocation problems (Ibaraki and Katoh, 1988; Shao and Rao, 2001), but it considers a variety of IT resource types for supporting specific IT functions, instead of general resources that can be allocated to any activity or agent.

Some topics are suggested for future research. The IT functions considered by our model are treated as separate and independent, which means there is no physical or logical link between any two IT functions. This assumption may have an effect on the granularity of IT assets being relatively large since finer-grained IT assets typically can serve multiple purposes. For example, a workstation may be used simultaneously as web server, database server, and email server to support IT functions of e-commerce transactions, data storage, and information communication, respectively. In future study, the proposed model can be extended to address interrelated IT functions by modifying the objective function. The approach of probabilistic dynamic programming would still be applicable for solving this extended problem (Berman and Ashrafi, 1993).

Moreover, we can categorize IT assets as hardware, software, human capitals, and other types to examine the impacts of specific characteristics of each IT asset type on the redundancy allocation decisions for disaster recovery planning. For example, tangible hardware cannot be duplicated without purchasing two equipments, but software with proper licenses can be easily deployed to many IT assets. Their costs implications thus are expected to be different. Another promising avenue would be to look at redundancy allocations at the industry value chain level and analyze disaster recovery planning across business partners in a coordinated and collaborative manner.

REFERENCES

1. N. Ashrafi and O. Berman. Optimization Models for Selection of Programs, Considering Cost & Reliability. *IEEE Transactions on Reliability*, vol. 41, no. 2, pp. 281-287, June 1992.
2. O. Berman and N. Ashrafi. Optimization Models for Reliability of Modular Software Systems. *IEEE Transactions on Software Engineering*, vol. 19, no. 11, pp. 1119-1123, Nov. 1993.
3. K. Bryson, H. Millar, A. Joseph, and A. Mobolurin. Using Formal MS/OR Modeling to Support Disaster Recovery Planning. *European Journal of Operational Research*, vol. 141, pp. 679-688, 2002.
4. I. Chengalur-Smith, S. Belardo, and H. Pazer. Adopting a Disaster-Management-Based Contingency Model to the Problem of Ad Hoc Forecasting: Toward Information Technology-Based Strategies. *IEEE Transactions on Engineering Management*, vol. 46, no. 2, pp. 210-220, May 1999.

5. M. Grabowski, J. R. W. Merrick, J. R. Harrald, T. A. Mazzuchi, and J. R. van Dorp. Risk Modeling in Distributed, Large-Scale Systems. *IEEE Transactions on Systems, Man, and Cybernetics-Part A*, vol. 30, no. 6, pp. 651-660, November 2000.
6. T. Ibaraki and N. Katoh. *Resource Allocation Problems*. MIT Press, MA, 1988.
7. R. K. Iyer and J. Sarkis. Disaster Recovery Planning in an Automated Manufacturing Environment. *IEEE Transactions on Engineering Management*, vol. 45, no. 2, pp. 163-175, May 1998.
8. L. Jenkins. Selecting Scenarios for Environmental Disaster Planning. *European Journal of Operational Research*, vol. 121, pp. 275-286, 2000.
9. W. Kuo and V. R. Prasad. An Annotated Overview of System-Reliability Optimization. *IEEE Transactions on Reliability*, vol. 49, no. 2, pp. 176-187, June 2000.
10. W. Lewis, Jr., R. T. Watson, and A. Pickren. An Empirical Assessment of IT Disaster Risk. *Communications of the ACM*, vol. 49, no. 9, pp. 201-206, Sept. 2003.
11. M. Pidd, F. deSilva, and R. Eglese. A simulation study for emergency evacuation. *European Journal of Operational Research*, vol. 90, pp. 413-419, 1996.
12. B. B. M. Shao and H. R. Rao. A Comparative Analysis of Information Acquisition Mechanisms for Discrete Resource Allocation. *IEEE Transactions on Systems, Man, and Cybernetics-Part A*, vol. 31, no. 3, pp. 199-209, May 2001.
13. H. Tamura, K. Yamamoto, S. Tomiyama, and I. Hatono. Modeling and Analysis of Decision Making Problem for Mitigating Natural Disaster Risks. *European Journal of Operational Research*, vol. 122, pp. 461-468, 2000.
14. W. L. Winston. *Operations Research: Application and Algorithms*. PWS Publishers, Boston, MA, 1987.