Computer Backup Pools, Disaster Recovery, and Default Risk

YEHUDA KAHANE, SEEV NEUMANN, and CHARLES S. TAPIERO

ABSTRACT: There is a growing popularity of computer backup pools, where a few members share the ownership, use or right for service, or a computer center. Such a center stands by to provide for the lost computing capacity of a member suffering a computer breakdown and disaster recovery. The efficiency of such a solution may be examined from various points of view, such as costs, response time, reliability etc. We focus on the reliability of such an arrangement. Two types of default risks are discussed: the probability that the center itself will break down when needed, so that it would be unable to provide service (this is similar to the traditional measure of a "probability of rain") and a "perceived probability of rain" (the probability that a member will be affected by the failure of the center). We borrow the concepts of probability of ruin from the risk management and insurance literature, in order to reach explicit relationships between these probabilities and the pricing of a mutual computer pool. It is shown that the membership fee for each participant must be a function of both the payments of all members and their loss (call for service) distributions, reflecting thereby the simultaneity of and mutual interdependence of members.

1. INTRODUCTION
The growing dependence of large organizations on their computers emphasizes the high loss potential in case of interruption in the normal operation of their computers. Interruption of the computer center's services may drastically affect the ability of the organization to function, and to serve its customers. The loss may be as much as the direct loss of hardware and/or software (see for example Krauss [1986], Datapro [1983]) and in extreme cases may cause a long-term consequential loss, perhaps even bankruptcy. The problems arising from the shutdown of a large computer center are especially complicated, due to the need for a special environment (large area, power, wiring, cooling, communications etc.), and due to the long lead and installation times of computer hardware. It is not surprising, therefore, that much attention is given to the protection of computer centers. The means of protection include physical means and financial instruments, such as insurance. Being indemnified for a financial loss through insurance is not always sufficient to compensate for other losses which are often more important, especially when the survival of the firm is at stake due to a breakdown of its computer center. Therefore, control of risk is often preferred over insurance arrangements.

There are numerous technical and administrative means to control the risk of physical damage to hardware and software. Data and software can be protected easily by appropriate storage of backup tapes and disks in another, separate, location. Other technological solutions (for example, dual processors)—usually based on some sort of physical backup and requiring a substantial investment—are being employed to protect hardware systems.

There is a variety of solutions for large computer backup centers (see, for example Reed [1980], McDonald [1966], Datapro [1983]). They differ by their response time, cost and reliability. Among the most common solutions are:

1. **Hot Backup** Maintaining an additional site, which operates in parallel to the main installation, and immediately takes over in case of a failure of the main center.
2. **Warm Backup** Maintaining another inactive site ready to become operational within a matter of hours.
3. **Split Site** Two installations (each somewhat smaller than a hot backup) are used. In case of emergency one center can keep the organization running by performing only jobs with high priority (Datapro [1983]).

* Risk management literature often emphasizes the need for a simultaneous optimization of risk financing (insurance and risk control such as pooling). Under certain circumstances, a firm would prefer one method over the other, whereas under other conditions a combination may be desirable. In this paper no attempt has been made to address these issues.
4. "Cold Backup" Maintaining empty computer premises ("empty shell") with the relevant support ready to accept the immediate installation of appropriate hardware. "Cold backup" is used when the recovery time is mainly affected by the need to install the infrastructure and support systems (electricity, communications, air conditioning, etc.), whereas the cost is mainly affected by the cost of the hardware [Reed [1980], Dentai [1980], Sullivan [1980]].

5. "Mutual Backup" This is a mutual agreement between two computer centers, operated by different firms, which decide to assist each other in case of emergency on the basis of "best efforts." This appears to be the least expensive, but also the least effective arrangement, especially when both firms operate with similar peak loads, and where each has only a limited excess capacity.

6. "Pooling" A solution which is gaining popularity is a pooling arrangement where a few members join into a mutual agreement concerning a computer center, which is standing-by to offer its services to any member suffering from interruption in its computer center. The idle computer center may be employed in the form of "cold" or "warm" backup. The center serves a pool of users, who share the ownership (or pay a certain membership fee to the owner of the facility). Such pooling is the focus of this paper.

In practice, such pools tend to serve members (users) similar in size and having similar needs, i.e., they all use computers of the same family. The differences in configuration of various members using the same basic family are typically insignificant as the equipment is standard and can be purchased off-the-shelf in case of need. Otherwise, configuration differences can be handled by having some slack capacity in the backup center, in terms of peripheral equipment (disk drives, terminals, etc.).

Such pools are based on the ability to simultaneously serve more than one member in need. The capacity of the center is then shared among the users. The ability to share is facilitated by appropriate system software, by security arrangements, and by relevant contingency planning. The sharing arrangement has to be agreed upon in advance, and established on the basis of membership fees. The fees are a function of the service required and the quality of protection offered. The quality of protection is a parameter often overlooked in the analysis of this solution, and thus will be the focal point of our analysis in this paper.

2. RISK CONCEPTS
The membership fee that each member is willing to pay depends on several parameters, such as the expected capacity loss, and the significance of the computing power loss to the member organization. The membership fee depends, of course, also on the reliability of the system in providing a true backup service to the member. It is surprising that these relationships have, to the best of our knowledge, neither been recognized in theory or practice. The purposes of this paper are therefore: (a) to analyze these relationships; (b) to formulate an explicit pricing formula relating these parameters and the appropriate membership fee; and (c) to enhance the understanding of certain tradeoffs which may affect the operation and functioning of computer backup pools, and may determine the size of the population they serve.

The analysis in this paper borrows the concept of probability of ruin and mutual insurance, from the risk management literature, in order to reach an explicit pricing formula. (See a recent paper on the failure of a mutual insurer by Tapiero, Kahane & Jacque [1986].)

The focus of our analysis is on the parameters affecting the willingness of organizations to join such a pool; we attempt to obtain an explicit relationship between the price the participating members are willing to pay for a given assumed probability of loss (due to the disruption of a computer center's operations), and the reliability of this backup center.

Loss-sharing arrangement contracts are often defined as transactions where members exchange uncertain "prospects" with certain ones at the cost of a "premium" (see Beard, Pentikainen and Pesonen [1972], Buhlmann [1970], Borch [1974]). In this context, the member faces no risk, once he has paid for the loss-sharing arrangement contract. Practically, however, there is always a tradeoff between the cost and the reliability of a backup service, which has to be considered by the potential participants and in the rate making process (Kahane [1979]).

The actual or perceived reliability of the backup arrangement may affect the participants' response to a particular membership fee policy. The optimal membership fee depends on the reliability (risk of failure) of the pool, which depends on the number of members participating in the pool (itself a function of the membership fee). The major contribution of this paper is the presentation and solution of this complex relationship.

In particular, we shall emphasize the similarity to the case of a mutual insurer, and introduce two notions of risk of failure, namely, the objective probability of the pool's being unable to provide service (due to breakdown, or its inability to serve the simultaneous calls for service from a number of members), and the perceived probability of the pool's default from the member's point of view (see also Tapiero, Kahane and Jacque [1986]). Thus, a member's decision may be guided by both the perceived, and the actual, probability of the pool's inability to serve the member. The paper assesses the effect of these two probabilities on the optimal membership fee.

The relationship between the membership fee and the risk of failure is analyzed in the following section, in which a model is presented and the risk of failure is defined and calculated. Particularly, we analyze a backup pool with N members (each being risk averter or risk neutral, and each facing a known risk, with at
most one call for backup service per member during the period).

3. THE POOL MEMBER AND THE RISK OF FAILURE

3.1 The Model. Consider a pool which backs up \( N \) computer centers, each with initial computing capacity \( W_i \) (this capacity, like other variables of the model, could be expressed either in terms of real capacity, or be translated into equivalent monetary values). Each member is exposed to two risks: the risk of complete or partial business interruption to its own facility, and the risk that the backup center defaults when its services are needed. Each participant has a "utility" function \( u(.) \) which describes its benefit from the available computing capacity. The utility from computing capacity is increasing, but at a declining rate \( u' = \beta_0 u(2) \beta_2 \geq 0 \). \( u' = \beta_0 u(2) \beta_2 \geq 0 \) implying an increasing absolute risk aversion, \( \beta_1 = -u'/u' > 0 \). \( i = 1, 2, \ldots, N \).

Each member \( i = 1, 2, \ldots, N \) is exposed to the risk \((p, \bar{X})\), where \( p \) is the probability of its computer center failure ("call for service") occurring within the period (at most one call for service is allowed per contracted backup period), and \( \bar{X} \) is the random variable describing the magnitude of the loss of computing power with known distribution functions \( F(\cdot) \). Each member pays a periodical membership fee \( M_i^* \) and these payments are used to purchase capacity in the backup center.

In practice, firms can often sustain a certain loss of computing capacity by simply deleting jobs with lower priority. Therefore, the model allows for the purchase of a "partial" protection. It is assumed that the backup center provides capacity on a proportional basis; for example, in case of a breakdown the member is entitled to be serviced for a loss of computing power of \((1 - \theta)\bar{X}_i\), and retains \( \bar{X}_i (1 - \theta) \), where \( \theta \) is a "loss-sharing arrangement" (coinsurance) factor.

Calls for service occurring within the period are answered on a first-come, first-served basis. The pool arrangement may, however, default when the available backup computing capacity is insufficient to cover all calls, or when a technical problem interrupts the backup center's services. The probability of this happening (the "probability of ruin") is denoted by \( R_i \).

It is possible that the backup pool will be unable to serve, and yet the individual member remains unaffected (since it has submitted no call for services, or since it received service prior to the depletion of the computer pool's capacity). The "perceived probability of ruin" measures the probability of the members being affected by the pool's inability to serve. This probability is a function of the number of calls for service, their sizes, and the order in which the calls for services have occurred.

For convenience, we summarize the model's notations in Table 1.

### Table 1. Notation

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>( i )</td>
<td>subscript denoting computer center (member)</td>
</tr>
<tr>
<td>( i = 1, 2, \ldots, N )</td>
<td>utility</td>
</tr>
<tr>
<td>( W_i )</td>
<td>initial computing capacity</td>
</tr>
<tr>
<td>( p )</td>
<td>probability of computer center failure</td>
</tr>
<tr>
<td>( x )</td>
<td>magnitude of capacity loss (stochastic variable)</td>
</tr>
<tr>
<td>( \theta )</td>
<td>proportion of the capacity loss being uninsured</td>
</tr>
<tr>
<td>( M_i^* )</td>
<td>membership fee (&quot;premium&quot;) measured in terms of capacity which could have been acquired for that price</td>
</tr>
<tr>
<td>( B )</td>
<td>the probability of backup center failure due to breakdown or due to excessive demand (call for service)</td>
</tr>
<tr>
<td>( A )</td>
<td>probability that a member will be affected by the backup center inability to serve</td>
</tr>
<tr>
<td>( q )</td>
<td>a &quot;loading factor&quot; (pool's costs)</td>
</tr>
</tbody>
</table>

Let \( A \) be the (conditional) probability that a member is affected by the pool's inability to serve. If \( \theta \) is the coverage ratio of the ith member, and \( E_{A_i}(\cdot) \) is the expectation operator over \( \bar{X}_i \) and \( p \), then its expected utility with the backup arrangement is given by:

\[
E_{u_i} = (1 - B) \sum_{i=1}^{N} U_i (W_i - M_i - \bar{X}_i) + B \left[ (1 - A) \sum_{i=1}^{N} U_i (W_i - M_i - \theta \bar{X}_i) \right] + A \sum_{i=1}^{N} U_i (W_i - M_i - \bar{X}_i) \quad (1)
\]

Since \( p \) is the probability of a call for service occurring, and \( 1 - p \) the probability of no call, i.e., \( X_i = 0 \), equation (1) yields the simpler expected utility (with \( E_{A_i}(\cdot) \) the expectation operator over \( \bar{X}_i \), the ith member service):

\[
E_{u_i} = (1 - p) U_i (W_i - M_i) + p (1 - B) \sum_{i=1}^{N} U_i (W_i - M_i - \bar{X}_i) + p B \left[ (1 - A) \sum_{i=1}^{N} U_i (W_i - M_i - \theta \bar{X}_i) \right] + A \sum_{i=1}^{N} U_i (W_i - M_i - \bar{X}_i) \quad (2)
\]

For a member to participate in pooling it is necessary that the expected utility (2) be greater than the expected utility of a "self-backup" arrangement, or

\[
E_{u_i} \geq p \sum_{i=1}^{N} U_i (W_i - \bar{X}_i) + (1 - p) U_i (W_i) \quad (3)
\]

[1] The membership fee, \( M_i^* \), is usually a monetary payment. However, it is more useful to measure it in units of capacity (i.e., the capacity which could be purchased for such a monetary payment).

[2] In practice, most centers will be fully covered for the loss of computing capacity, thus \( \theta \approx 0 \) in most cases. The model in this paper allows, however, for the more general case of \( 0 < \theta \leq 1 \).

[3] This enables handling cases where the member is protecting only a certain percentage of its capacity, knowing that in case of emergency certain low priority jobs could be terminated.

[4] In practice, such a case appears will be requested to run non-critical, and low priority jobs. Therefore, assuming an inflexible case of "all or nothing" makes the model somewhat unrealistic. An interesting issue which is deferred to another study is appropriate pricing formula. This will enable users to more effectively compete for the backup center services by offering higher marginal payments for their more valuable applications.
From equation (2), we note that $E_W$ is expressed in terms of the default probability $B$ of the computer backup pool and by the perceived (conditional) probability of default, both a function of the membership fees $M_i$, $i = 1, 2, \ldots, N$ paid by members, their coverage ratio ("coinsurance rates") $\theta$, as well as other parameters, such as the pool’s initial capacity $W_0$, the loss severity distribution, the statistical dependence among risks etc. The level of the membership fee will be determined as the result of the simultaneous decisions made by all members taking into consideration all these parameters—thus, its computation can be quite complex.

Assume that $A_i$ is the $i$th member’s conditional probability of being affected by the backup center’s default (if it occurs). In this case, equation (3) [together with (2)] can be solved for the fee and the probability of default. Straightforward computation yields:

$$AB \leq \frac{(1 - p)[pU(W, M) - U(W)]}{E[U|W, M, \theta, X] - E[U|W, X]}$$

where $\theta$ is the coverage ratio, $\theta = 1, 2, \ldots, N$; the product "A,$\theta$" is the unconditional probability of default as assessed by the $i$th member. This default probability is, of course, the one relevant for computing the appropriate level of backup service and the membership fee. It can be expressed as a function of the information available to the member regarding the reliability of the mutual backup arrangements, other members’ risk, the statistical dependence of these risks etc. Thus, $A, \theta$ is a function which would generally be written as:

$$A, \theta = \gamma_1(M_i, \ldots, M_N, \theta_1, \ldots, \theta_N; \text{other parameters})$$

expressing the complexity of the decisions concerning the appropriate membership fee. Simple cases can, however, be used to obtain some insights regarding the relationship between the probability of the pool’s failure faced by the member and the membership fee. Several cases are examined below.

CASE A. Homogeneous Risk Neutral Members. Let all pool members be homogeneous and with linear (risk neutral) utility function $U(x) = x$. Then, equation (4) is reduced to

$$AB \leq \frac{|pX(1 - \theta) - M|/|X(1 - \theta)|}{(1 - p)}$$

where $X = E[X]$, $\theta \in [1, N]$. When the inequality sign is replaced by equality, we obtain an expression for a "fair" membership fee ("actuarially fair premium"). Since $AB$ is necessarily a function of both $N$, $M$, $\theta$, and the distribution of the severity of the interruption, a fair fee $M$ is more complex than might be expected by just looking at equation (6). It is only in the special case of a "risk free" pool ($\theta = 0$), that $M \leq p(1 - \theta)/\gamma$, which is analogous to the well-known condition for actuarially fair insurance premiums. In the more general case, when $AB > 0$, it is evident that the membership fee is smaller than in the (hypothetical) case of a pool which is guaranteed to be risk free.

In this special case ($1 - \theta)$ $AB$ can be interpreted as the fee the member is willing to pay to be insured against the default risk.

CASE B. Homogeneous Members with a Quadratic Utility. When all the members are homogeneous and have a quadratic (risk averse) utility function, such that $EU(Z) = E(Z) - \frac{1}{2} \sigma(Z)^2$, where $\sigma$ is a parameter of risk aversion then:

$$AB \leq \frac{(1 - p)[pU(W, M) - U(W)]}{E[U|W, M, \theta, X] - E[U|W, X]}$$

where $\sigma$ is the mean and variance, respectively, of the call for service if it occurs.

If $AB = 0$, we again obtain a standard and well known result for a fair fee, which increases due to the member’s aversion to risk and its severity variance. This fee will decrease as a function of the coverage ratio $\theta$; however, when $AB = 0$, then $X(1 - \theta)$ $AB$ is again the fee the member might be willing to pay to be insured against the default risk.

CASE C. Exponential Utility (Constant Risk Aversion). Now assume that the members’ utility is of the constant risk aversion type (for example, exponential), with risk parameter $\beta$. The fair fee is found by

$$\min \leq \frac{(1 - p) - pG(\beta)}{(1 - p) + pG(\beta) + AB[G(\beta) - G(\beta)]}$$

where $G(\beta)$ is the moment generating function (E $\exp(\beta X)$) of the loss severity distribution. The fair fee $M$ can be computed again (with difficulty) since $AB$ is a function of $N$, $M$ and the various parameters which affect the financial wealth of the pool.

In order to characterize such a distribution we shall assume that the backup pool has an initial capacity $W_0$ and that it collects a total fee of $NM$ at the beginning of the period. The fee paid by each member is determined by

$$M = (1 + \phi)E[X]$$

where $\phi$ is the charge to cover the pool’s costs ("loading factor") used by the pool (Tapiero 1984). Tapiero, Zuckerman, and Kahane [1983]. Further, we shall assume that all members are homogeneous and all have complete information regarding one another. These restrictive assumptions will considerably simplify the computation of the default risk below.

3.2 The Perceived Default Risk and the Probability of Ruin. Pooling is viewed as a collective process where $N$ members, each paying a fee $M$, and selecting a coverage rate ("coinsurance") $\theta$, are mutually "insured" against any losses covered by the contract, contingent on the pool’s ability to meet the calls for ser-
vice. At the beginning of the period, the pool’s capacity is
\[ W_0 + \sum_{i=1}^{N} M_i \]  
(10)
where \[ M_i = (1 + q)p E(X_i)(1 - \theta) \].
Here, \( E(X_i) \) is the total expected call for service, \( p \) is the probability of a call, \( \theta \) is the call rate, and \( q \) is the loading factor applied uniformly to all members. For homogeneous members, \( M = M_i, p_i = p, \theta_i = \theta \) and \( E(X_i) = X_i, X_i \in [1, N] \) and the pool’s initial capacity is
\[ W_0 + N[(1 + q)p X(1 - \theta)] \].
Now let \( j \), a random variable, be the number of calls for service which occur during the period, each call giving rise to a loss of \( X_i \), \( k = 1, 2, \ldots, j \) with identically and independently distributed severity with density function \( f_j(\cdot) \). Denote by \( h(j) \) the probability distribution of \( j \), and by \( S_n \), the probability of the backup center being down (or exhausting its capacity), after the \( n \)th call. It follows that:
\[ S_1 = 1 - F_1(\delta) \]
\[ S_2 = F_1(\delta)[1 - F_2(\delta)] \]
\[ \vdots \]
\[ S_n = \prod_{k=1}^{n} F_k(\delta)(1 - F_k(\delta)) \]
where \( F_k(\cdot) \) is the cumulative distribution of the sum of \( k \) calls, each independently and independently distributed with distribution function \( f_k(\cdot) \). Thus, the probability of default \( R \) is simply given by:
\[ R = \sum_{j=1}^{n} h(j)S_j \]  
(12)
which is the expectation that \( j \) calls occur and the probability event that default occurs after the \( n \)th call, \( m \rightarrow j \). The expected number of calls which are not serviced due to default, is also given by:
\[ \sum_{j=1}^{n} h(j)S_j \]
(13)
This is the expected sum of the number of calls \( j \), less the event that default occurs at the \( n \)th call. If all members have equiprobability of a call occurring and \( j \) calls occur (while default occurs after the \( n \)th call), then \( 1 - n/j (j > n) \) is the probability that the member will not be covered when default occurs. In other words, the unconditional default risk is
\[ AB = \sum_{j=1}^{n} (1 - n/j)h(j)S_j \]  
(14)
This latter expression is an estimate of a member’s perceived probability of default in this mutual backup agreement. Combining this equation with (4) and an appropriate (say binomial) distribution for \( h(j) \), we obtain explicitly:
\[ AB = \sum_{j=1}^{n} (1 - n/j) h(j)S_j \]
\[ = \prod_{j=1}^{n} F_j(\delta)(1 - F_j(\delta)) \]
(15)
where
\[ \delta = [W_0 + N(1 + q)p X(1 - \theta)]/(1 - \theta) \]
and for a “fair” loading factor \( q \) when the utility is of the mean-variance type (equation (7)) for example:
\[ (1 + q) \leq 1 + \Pi(1 + \theta)(\delta_c/\delta) \]  
(16)
which is solved for \( q \) by inserting \( AB \) from (15) into (16) and replacing the inequality sign in (16) by an equality sign to obtain the actuarial loading factor \( q \).
Define the implicit function
\[ Q = (1 + q) - 1 + (1 + \theta)(\delta_c/\delta) \]  
(17)
Then by implicit differentiation we can assess the sensitivity of the required fair fee with respect to each of the parameters in (17). For example, \( \delta_c/\delta = -[\partial Q/\partial \theta]/[\partial Q/\partial q] \) and
\[ \frac{\partial Q}{\partial \theta} = \frac{\partial Q}{\partial \theta} \]
\[ \frac{\partial Q}{\partial q} = \frac{\partial Q}{\partial q} \]
(18)
If \( \partial Q/\partial q < 0 \), we can infer the relative effects of \( q \) and \( \theta \) on the default probability. Due to the complicated functional form of \( AB \) (equation 15) this is a difficult task which can be accomplished by numerical analysis.
For a risk neutral member, it can be shown that \( q \leq -AB/p \), or the loading factor is slightly negative, expressing a default risk which is assumed by the member when joining into this mutual arrangement. In other words, the default risk will tend to reduce the fee the member might be willing to pay to enter into this mutual pooling arrangement. This relationship will be increased further when risk aversion is taken into account, implying that \( q(\Pi) < q(0) \), or the loading calculated by (17) will be bounded by \( q(0) = AB/p \). It follows that the smaller the default risk, the larger the fee each member is willing to pay.
In case of a mean variance utility function (equation 17), a simple linear relationship is obtained:
\[ \frac{\partial Q}{\partial AB} = \frac{1}{1 + \Pi(1 + \theta)(\delta_c/\delta)} \]
(19)
This simple equation provides the net effect the default risk has on the member’s willingness to pay or on the loading factor. For example, if we reduce the probability of the member’s perceived default by (say) 20 per-

January 1988 Volume 31 Number 1

Communications of the ACM
cent, then $\Delta B = -2$ and the incremental change in the loading factor is

$$\Delta \theta = 2(1 + \theta)(\theta/\sigma/X)(1/p)$$

This increment is an increasing function of $\sigma^2$, $\theta$ and $\theta$, and a decreasing function of $\theta$ and $X$, respectively.

4. CONCLUSIONS

This study was intended to add insights and enhance the understanding of some interesting tradeoffs which exist in the choice of the optimal size (number of members served) of a computer backup pool, and the appropriate membership fees (= insurance "premiums"). Our results point out explicit tradeoffs and relationships between the default risk and fees required of members of a mutual computer backup pool.

Such relationships have not been investigated previously in the computer literature. When the number of members is large, risks tend to be very large (and possibly correlated), and the default risk might become considerable.

Under such circumstances, our analysis points out formulas which can be used to compute optimal membership fees. Due to the complexity of the model, explicit relationships may be obtained under certain restrictive assumptions. More realistic cases have to be analyzed with the aid of numerical analysis.

Other properties of the analysis point out the effects of parameters which tend to justify higher membership fees (for example, the variability of a computer center suffering a loss, the members' aversion to risk, and their willingness to "self insure" parts of the risk). On the other hand, the probability of loss, and the size of such a potential loss tend to reduce the loading factor, and hence the fees.

There are several problems of interest related to this paper which were not discussed, such as: the use of pooling arrangements among the pools themselves (similar to reinsurance arrangement in commercial insurance) in reducing (or perhaps eliminating) the default risk for members, the use of different types of computers, the use of insurance, the effects of information symmetry and members' heterogeneity on fees and default risk, and so on. These are problems which we hope to pursue in future research.

Acknowledgments. We would like to thank the editor and anonymous referees for their helpful comments and suggestions. All the usual caveats apply.

REFERENCES


CR Categories and Subject Descriptors: K.6.0; K.6.2; K.6.4.

Additional Key Words and Phrases: Backup, claims process, computer failure, computer risk management, membership fee, pooling, portfolio, probability of ruin, utility

Received 8/86; revised 6/87; accepted 9/87

Authors' Present Addresses: Yehuda Khabani and Sven Neumann, Faculty of Management, Tel Aviv University, Ramat Aviv, Tel Aviv, Israel 69978; Charles S. Tapies, Graduate School of Business, Hebrew University, Jerusalem, Israel.

Permission to copy without fee all or part of this material is granted provided that the copies are not made or distributed for direct commercial advantage: the ACM copyright notice and the title of the publication and its date appear, and notice is given that copying is by permission of the Association for Computing Machinery. To copy otherwise, or to republish, requires a fee and/or specific permission.