

# An Empirical Assessment of IT Disaster Risk

WILLIAM LEWIS, JR., RICHARD T. WATSON, AND  
ANN PICKREN

Disasters have historically been associated with catastrophic events such as floods, fires, hurricanes, or earthquakes, but recent computer failures, such as the air traffic system failure at Washington Center, have broadened the definition of disaster—as any event causing significant disruption to operations, thereby threatening business survival [9]. With the incentives of cost-efficiency and competition driving business to place more critical information assets into automated systems and networks [4], the loss or denial of assets required for normal operations can have a catastrophic impact on a firm's bottom line [2]. Such disasters may involve the loss of integrity or reliability in a critical dataset or in the means by which data are transported, manipulated, or presented.

As firms grow more dependent on uninterrupted information system functioning, disaster recovery (DR) is receiving increasing attention, and a growing number of organizations are beginning to engage in DR planning. In addition to cold sites, reciprocal agreements, and other services, DR vendors market a service known as “hot sites,” designed to provide standby computer resources in the event that one or more subscribers require an alternative computer center to process critical applications. Companies pay steep monthly subscription fees for hot-site facilities, into which company departments can move, literally overnight, if required [6]. This requirement is usually prompted by an actual or perceived event that could render the subscriber's computer systems inoperable. The activation of hot site service is initiated through the formal declaration of a disaster. The definition of disaster varies by client, with hot site providers generally allowing a broad interpretation of the term. For example, some vendor clients declare disasters in order to provide backup data processing capability during a planned relocation of their data center.

Despite the vital necessity of uninterrupted IT capability for most of today's organizations, few empirical studies provide practitioners and academicians with a

---

**WILLIAM LEWIS, JR.** (wlewis@terry.uga.edu) is an assistant professor of Management Information Systems at Terry College of Business, University of Georgia, Athens.

**RICHARD T. WATSON** (rwatson@terry.uga.edu) is the J. Rex Fuqua Distinguished Chair for Internet Strategy, Director of the Center for Information Systems Leadership (CISL), Management Information Systems, Terry College of Business, University of Georgia, Athens.

**ANN PICKREN** (aspickren@comdisco.com) is Senior Vice President of SunGuard Planning Systems, Wayne, PA.

---

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

---

better understanding of the causes and impacts of IT disasters. In this article, we analyze 19 years of disaster recovery data, with the goal of giving organizations a foundation for system design strategies to ensure business continuity.

## Risk Management

Many activities undertaken by organizations do not have predictable outcomes; one can't predict the return from a new project, for example. As such, occurrence of these types of events can only be described in terms of a range of possible outcomes and the likelihood or probability of each outcome. The lack of predictability of outcomes is referred to as risk. The concept of risk does not imply all possible outcomes are adverse, only that the precise probabilities of the outcomes are unknown [1]. Risk management concerns the management of events, usually adverse in nature, which cannot be predicted. The overarching objective of risk management is to purchase coverage for enough insurable perils that managers are free to focus on the central affairs of business [7]. Some risks faced by the firm are either so remote, such as data center destruction by meteorite impact, or so routinely small, such as a corrupted floppy disk, that they are minor concerns to managers. Between these two extremes lie risks of sufficient probability and severity to impose significant threat and uncertainty [1]. These losses are the primary focus of corporate risk management activity (see Figure 1). Risk managers use statistical techniques based on probability distributions (such as normal, bimodal, and Poisson) to develop quantitative estimates of the frequency and severity of hazards facing the firm, to determine precisely how much coverage the firm should purchase.

The rapid development of new technologies means new risks—with an insufficient history to base premium rates on—now comprise a larger proportion of all risks [3]. In many companies, responsibility for managing technology risk now falls between the purview of two functions: The IS unit and the risk management department. Partnering with the IS department, which is well versed in technology but not trained to assess organizational risk, helps remove some of the mystery from technology-related risk so familiar risk management approaches can be applied [4, 8].

Claim frequency and size are two components that must be considered when calculating the risk premium, which is the amount needed to meet the expected cost of the risk covered, sans management fees and other overhead expenses [3]. Only in rare

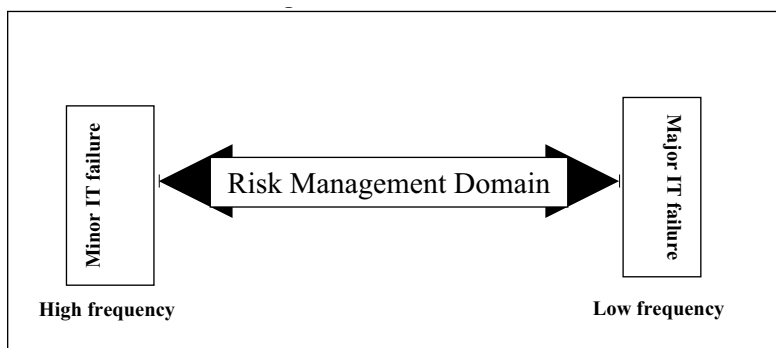


Figure 1. IT disaster risk.

cases should claim frequency alone be used to calculate risk premium. Most factors affect frequency and size differently. For example, an upgrade to a hard drive with more storage capacity may have a small effect on the frequency of drive failures within a given time period, but any potential data loss would be more sizable than with a smaller drive.

The increased use of IT for vital business processes has facilitated the growth of a new economy. Yet, dependence on technology holds the potential to bankrupt an organization. Generally accepted analysis techniques used in risk management can be applied to IT to help meet this challenge. An analysis employing such techniques can provide a risk profile to identify specific disruptive events, business segments, locations, individual policies, or contracts that contribute disproportionately to overall loss potential. Such an analysis can reduce uncertainty and support better strategic decision-making [10].

### IT Disaster Risk

For the purposes of this article, a major international provider of disaster recovery services supplied data on all disaster recovery events experienced by the firm's clients from 1981 to 2000. The firm had a market share of 38% when it supplied the data, and it provided services to at least seven of the top 10 companies in a range of industries. Thus, we believe it is reasonable to assert the data are representative of disaster incidents. A total of 429 disaster declarations were reported during that time. The data collected for each disaster included a description of the disruption, the recovery facility used by the client, the type of computer equipment utilized in the recovery, and the number of days the client occupied the hot site facility.

The firm's customers declared IT disasters for a variety of reasons. In one case, an intense freeze caused a water main to burst, flooding the computer room and destroying all equipment. That customer occupied a hot site for 45 days. In another incident, an air conditioning failure caused the temperature in a client's computer room to exceed the safe operating range of the equipment, resulting in a one-day hot site occupation. Another customer declared a disaster due to the threat of an approaching hurricane in a coastal region and occupied one of the recovery facilities for two days. In order to provide a conceptual basis for analysis of the incidents, the causes for all the disasters were carefully reviewed and grouped into 14 categories. Table 1 lists the seven disaster categories that occurred most frequently along with their

Category	Description
Disruptive act	Worker strikes and other intentional human acts, such as bombs or civil unrests, designed to interrupt the normal processes of organizations.
Fire	Electrical or natural fires.
IT failure	Hardware, software, or network problems such as DASD failures or bad controller cards.
IT move/upgrade	Data center moves and CPU upgrades undertaken by the company that cause disruption.
Natural event	Earthquakes, hurricanes, severe weather (for example, heavy rains or snowfall) or other events that lack dependence on human activity.
Power outage	Loss of power.
Water leakage	Unintended loss of contained water (for example, pipe leaks, main breaks).

**Table 1.** Most frequent IT disasters.

Category	N	Min.	Max.
Natural Event	122	0	85
IT Failure	98	1	61
Power Outage	67	1	20
Disruptive Act	29	1	97
Water leakage	28	0	17
Fire	22	1	124
IT Move/Upgrade	14	1	204
Environmental	6	1	183
Miscellaneous	5	1	416
IT Capacity	2	4	8
Theft	2	1	3
Construction	1	2	2
Flood	1	13	13
IT User Error	1	1	1

**Table 2.** Days of disruption per year.

descriptions. Table 2 lists the frequencies and minimum and maximum days of disruption for all the categories.

While frequency data provides useful information about the occurrence of different types of disasters, managers also need quantitative assessments of the level of severity associated with these events in order to better manage the IT function. The theory of risk, a branch of actuarial mathematics that incorporates the study of the random fluctuations of accumulated claim amounts [3], is a useful guide to the general order of magnitude of various risks faced by the corporation. The technique uses the standard deviation of the accumulated claim amount as an indication of the relative risk of the holdings of a portfolio. Riskier holdings have a greater amount of dispersion in claim amounts. The formula used to calculate relative risk is:

$$[c^2 * p - (c * p)^2]$$

where c = claim amount; p = probability of claim

This technique can be used to assess the relative risk for different causes of IT disruptions. Since the level of risk calculated using the formula is relative, accumulated days of disruption for each type of disaster serves as a valid proxy for claim amount. Probabilities for each type were calculated using the total number of declarations that occurred in the data period. Risk levels for each category were then calculated using the formula.

Based on the risk values in Table 3, natural events and IT failure appear to be by far the riskiest causes of IT disruptions. Disruptive behavior is approximately 15 times more risky than equipment moves or upgrades. Power outages and fire are seven and two times as risky as IT changes, respectively. The water leakage category had the lowest relative risk of the seven major types of disasters.

Disaster Category	Relative Risk
Natural Event	79.1
IT Failure	69.7
Disruptive Act	32.9
Power Outage	14.2
Fire	4.5
IT Move/Upgrade	2.1
Water Leakage	0.22
Miscellaneous	2.8
Environmental	2.4
Theft	0.0
Flood	0.0
IT Capacity	0.0
IT User Error	0.0

**Table 3.** Relative risk of IT disasters (in thousands).

## Conclusion

The strategic design of information systems should include hardware, software, and network solutions that minimize the impact of IT disasters. The increasing need for uninterrupted information processing capability makes IT availability vital for corporate survival. Hence, companies need to consider their potential exposure to IT disruption during the analysis and design stages of system development. For example, firms headquartered in regions where severe weather is not uncommon should be conscientious about designing systems and recovery plans that expedite resumption of normal business activity in the event of that type of disaster. Similarly, corporations whose business activities rely heavily on complex equipment, software, and networks should design systems that are more robust to technological failure. We urge all firms to review the recommendations of the Disaster Recovery Institute International [5]. The relative risks of the different categories of IT disruptions identified in this study can provide guidance in the design and implementation of strategic system solutions that avert or minimize corporate IT exposure and help ensure business continuity.

## References

1. Doherty, N.A. *Corporate Risk Management: A Financial Exposition*. McGraw-Hill, New York, 1985.
2. Glennen, A. Computer insurance—the only constant is change. *Insurance Brokers' Monthly and Insurance Adviser* 47, 12 (1997), 11–13.
3. Hossack, I.B., Pollard, J.H., and Zehnwirth, B. *Introductory Statistics With Applications in General Insurance*. Cambridge University Press, Melbourne, Australia, 1983.
4. Hughes, M.L. *Technorisk: Who's Responsible?* New York, 1997.
5. International, D.R.I. (2002). Professional practices for business continuity planners: Subject Area 2—Risk evaluation and control, Disaster Recovery Institute International. [www.drii.org/pparea2.htm](http://www.drii.org/pparea2.htm)

6. Jacobs, J. and Weiner, S. The CPA's role in disaster recovery planning. *The CPA Journal* 67, 11 (1997), 20–24.
7. Mehr, R.I. and Hedges, B. *Risk Management in the Business Enterprise*. Irwin, Homewood, IL, 1963.
8. Pelland, D. Several trends influencing risk management: future success stories? *Risk Management* 44, 12 (1997), 72.
9. Rothberg, M. L. Disaster plans-added complexity. *Computer Decisions* 21, 2 (1989),16–16.
10. Smith, J. M. Reducing uncertainties with catastrophe models. *Risk Management* 47, 2 (2000), 23–27.