Data Storage in the Worst of Times

Thomas M. Coughlin* and Farid Neema+
*Coughlin Associates
+Peripheral Concepts, Inc.

Data has always been at risk from natural disasters and human errors. Ever more rampant malicious hacker attacks and the threat of terrorist action against commercial interests further increase the risk to critical corporate data storage. What can be done to protect companies from the ravages of human and natural catastrophes?

Survey Background

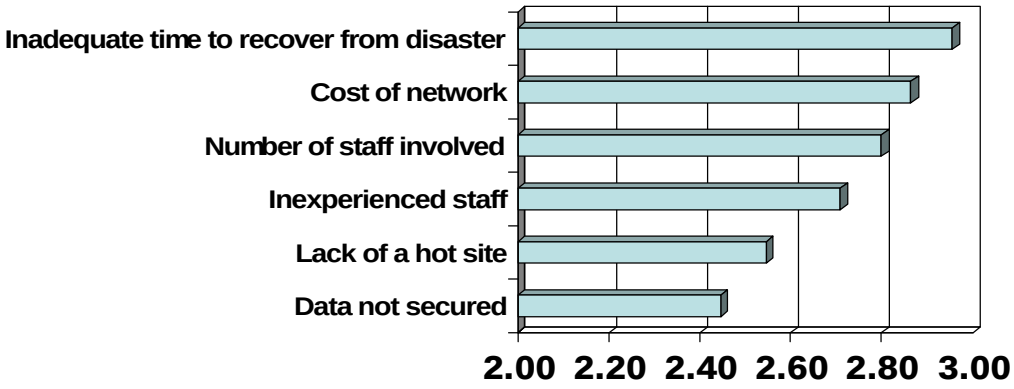
This article like the previous one is based on a survey of North American IT managers that was conducted from May through July of 2004. Parts of this article will appear in an issue of Computer Technology Review.

Risk and Costs of Downtime

Over one half of the respondents estimate that their entire company could be at risk if they are unable to recover critical data within 8 hours. 24% say that they could lose over $100,000 per hour of downtime. Despite this risk 17% of the surveyed population do not have a disaster recovery facility today,

The survey participants reported that inadequate time to recover from disaster was the biggest problem that they saw in disaster recovery and business continuance followed by cost of network, staff related issues, lack of a hot site, and data not secured as shown in **Figure 1**.

Figure 1. Problems in Disaster Protection and Business Compliance (5 = major problem, 1 = no problem, 0 = don't know or no opinion)

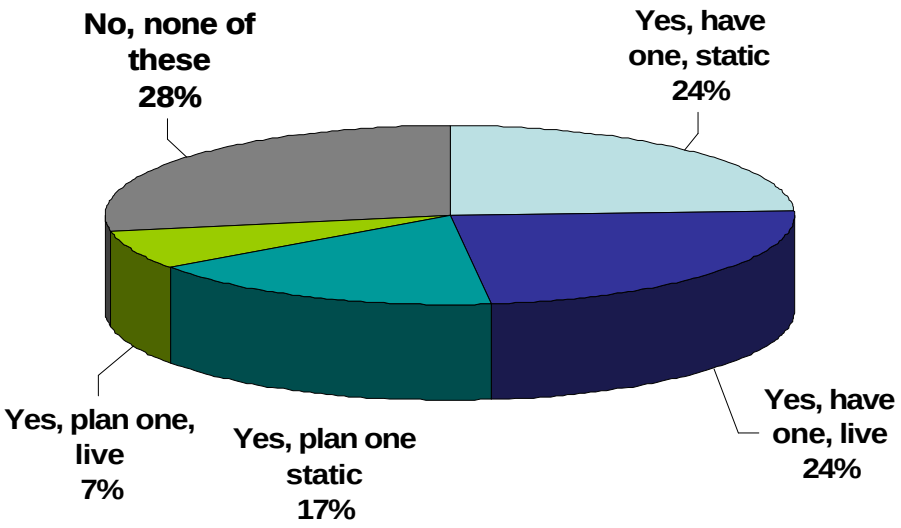


Data Protection Implementation

With close to one half of the sites having implemented remote replication, the Finance / Banking industry is the largest user. In general the number of IT sites using remote replication will more than double in the next two years, with Telecom and Health showing the highest growth.

Almost half the IT sites have implemented either a static or live hot site and another 24% have plans to implement a hot site within 2 years, see **Figure 2**.

Figure 2. Hot Site - Status and Plan



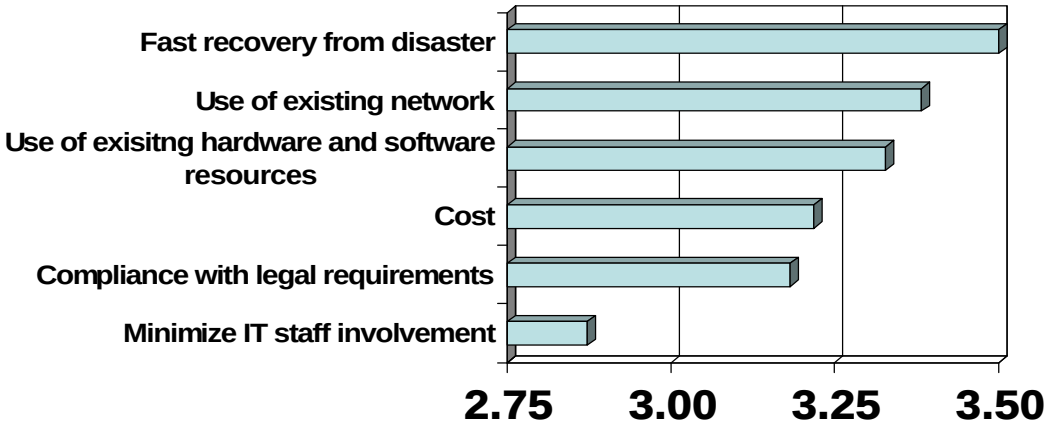
The number of sites utilizing multiple levels of data protection for different applications has more than doubled in the past 24 months and is poised for significant additional growth. In terms of features or techniques, disk-to-disk backup and SAN backup are the most widely implemented; remote replication, virtualization and IP storage stand out as the highest growth market potential.

What Do Customers Want and What Makes them Buy?

Data security is a growing concern with the extended use of networks in general, and of storage networking, in particular. While very few use encrypted data on their storage media today, 45% believe it is a needed feature.

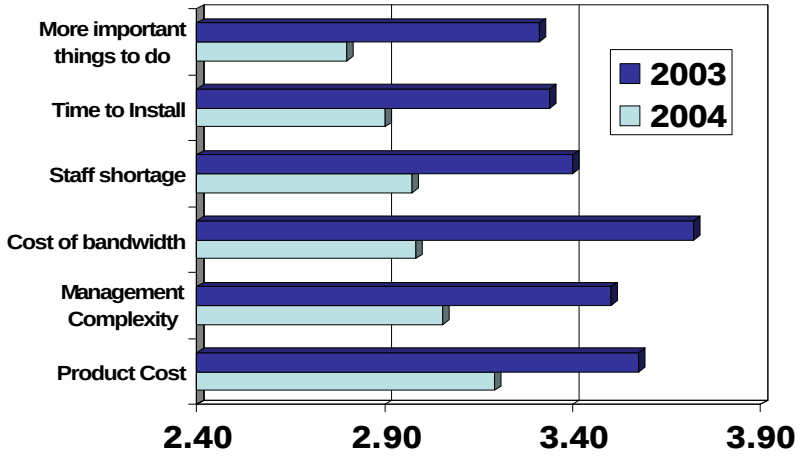
It is interesting that although cost follows behind fast recovery from disaster, use of existing network, and use of existing hardware and software resources as the criteria for selection of a business continuance solution (**Figure 3**) it ranks as the top impediment to implementation of data protection (**Figure 4**).

Figure 3. Criteria For Selection of Business Continuance Solution (5 = very high, 1 = very low, 0 = don't know or no a criterion)



While performance and utilization of existing resources are important considerations in selecting a business continuance solution purchase price is a major obstacle to actual purchase and implementation. The spirit is willing but the pocket book resists!

Figure 4. Impediments to Implementing Data Protection (5 = very high impediment, 1 = very low impediment, 0 = no opinion)



For More Information

The full **Business Continuance and Disaster Recovery--A User Perspective** report contains 143 figures summarizing site, industry, and revenue characteristics of the surveyed population as well as information on business continuance and disaster recovery plans, recovery point and recovery time objectives, costs of downtime, as well as trends and perceptions. The report can be ordered from www.tomcoughlin.com (see Technical Papers section on web site). A companion report based on the survey is also available covering Backup and Archiving.