

Business Continuity and Information Technology

A Primer for Disaster Recovery Planning

I. SUMMARY

As companies become more dependent on the Internet for customer orders, customer communication and business applications, their data and computing infrastructure have become mission critical. A recent Gartner Group study highlights this fact: 40 percent of all businesses that lose their data in a disaster go out of business within 5 years.

Today's organizations are quickly coming to grips with the very real risks that the failure of their IT systems pose to the viability of their business. The risks not only include the failure to comply with mandatory regulations but also the interdependency and reliance of systems and their potential impact on the business operations. Organizations of all sizes are moving to identify their risk exposure in terms of their IT interdependencies and establish clear policies and procedures to eliminate or minimize the impact that IT systems failure can have both operationally and financially.

The purpose of this paper is to provide a high level "risk model" for organizations to better manage their IT risks. This document also provides guidelines on how to measure risk in an environment with the very real possibility of both minor and major disruptions to their IT services.

II. DEFINING RISK – WHAT'S AT STAKE

There are a number of ways to define risk as it pertains to an organization but for the purpose of this document we look at the risks in terms of impact on your business. These risks have significant, potentially incalculable real and intangible costs. Some examples are:

A. Loss of Cash Flow

Most organizations rely to some degree on their IT to generate revenue and collect cash. If you were to immediately, without notice, shut down all your computers and remove access to data, would there be any effect on cash? There's also the negative impact to cash flow resulting from the increased expenses required to employ "work around" processes and staff overtime to continue operations for remediation and restoration.

B. Regulatory Compliance

Some businesses, such as hospitals, require accreditation or operate under strict regulations. These organizations risk losing their accreditation or failing to comply with important regulations in the case of an IT disaster. These failures to comply can be extremely expensive if not detrimental to the organization.

C. Lost Customers

In highly competitive environments the risk of customer loss can be very high in the case of an IT disaster. Without your IT can you still service customers? If they can easily and quickly switch will they? For businesses like radio stations or websites where customers can go to your competitor with a mouse click, a prolonged IT outage can cause customer loss.

D. Damaged Brand

Outages or major disruption to your business can cause customers and prospects to lose confidence in your brand. An investment in your "Brand" provides return in that it gives customers confidence in you. Major outages obviously can shake confidence in a company much more quickly than it takes to build it up.

E. Demoralized Staff

Long recovery times following a major disruption to systems can have a negative and sometimes debilitating effect on IT staff due to the long hours required for problem solving and restoration efforts. Adding to the impact is the need for this very same staff to maintain any and all systems that were not affected by a disruption while recovering effected systems.

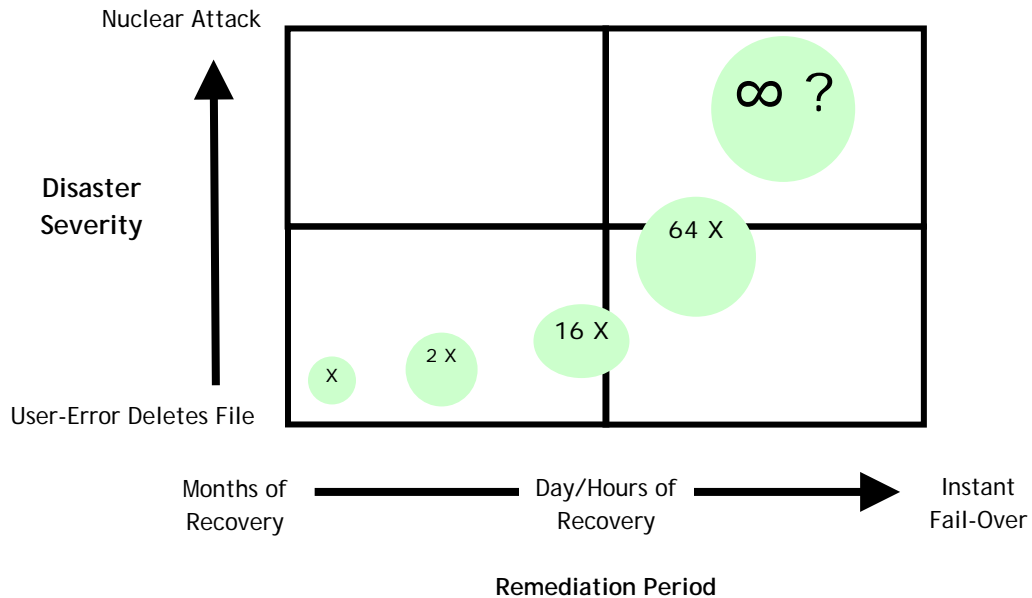
III. MEASURING YOUR RESPONSE TO RISK

Risk is truly a relative term and means different things to different areas of the enterprise.

From a pragmatic viewpoint, there is a vast spectrum of severity that disasters can wreak – from a single server failure to a tornado ravaged data center to a nuclear attack.

Independent of severity is the question of time to remediation. How fast and to what degree do you need to be able to recover from the various levels of severity? It would be ideal to be able to recover immediately from the most severe disasters. In reality, the cost of remediation goes up with the severity of the disaster and the required recovery time.

The grid below depicts these two independent variables and provides a framework to develop a disaster recovery strategy.



As you move from the lower left corner to the upper right corner, the costs go up exponentially. Almost universally, the opportunity to invest in protection against ever-greater severities with ever faster remediation time is practically infinite. The challenge then becomes deciding from what level of severity you want to recover and to what degree. Ultimately this is the process of arbitraging risk. So what *level of risk* should you accept?

IV. ACCEPTABLE RISK LEVELS AND BUDGETING

Risk is inherent in any entity. The objective is to budget appropriately for risk given your specific situation. So, what is *appropriate*? It's as easy to over-spend as it is to under-spend. If you over-spend, you risk wasting capital, or the perception of wasted capital. If you under-spend and a disaster occurs, you risk very high degrees of liability, and potentially the survival of your business.

Online Tech uses a methodology that looks at your Disaster Recovery needs from two different perspectives. You can use them together to determine the appropriate spending levels and to start building a detailed budget. The two perspectives are:

- 1) Top-Down: A top down analysis of Disaster Recovery budgets reveals a ration of spending to total IT budget. This top down analysis, based on industry assumptions

and benchmarks provide useful distant goalposts. Budgets that vary significantly from these raise flags, regardless of the other two analyses.

2) Bottom-Up Summary: Bottom up analysis provides a detailed list of one-time and recurring tasks and items that are required to provide DR for the critical systems with broad reach. This information, while not necessarily accurate at the task level, provides a start for building detailed budgets and plans for implementing Disaster Recovery plans.

How do we integrate these analyses?

The Top-Down analysis is driven by a few basic financial and operating ratios. DR budgets from the top-down are expressed as a ratio of overall IT spending. As you spend more on IT you'll need to spend more to implement Disaster Recovery plans for your IT investment.

The Bottom-Up Summary provides details on the impact, mitigation strategy and mitigation budget for your key systems. This information is generally based on summary discussions with IT staff but ultimately requires further detailed interviews of non-IT staff to complete this analysis.

V. CONCLUSION

As companies become more dependent on their computing and data infrastructure for their business needs, business continuity depends more and more on how well the business recovers from disasters that impact their data centers.

One needs to assess the risks to the business for the various levels of threat and the cost to mitigate those risks when developing a Disaster Recovery plan. Low impact environments with relatively long recover time objectives (days) may be adequately served with weekly tape back-up stored off site. Those with mission critical systems such as financial services, e-commerce companies, or health providers where recovery time from major disasters in on the order of minutes or hours, need more sophisticated Disaster Recovery plans. Such DR plans might include geographically separate data centers running on separate power grids with different network providers, to assure no single point of failure in the case of a disaster.

Online Tech understands that each business is unique in its requirements and risk profile, and offers a broad range of solutions that meet most companies' needs. Call us and ask us about how we can help you with your Disaster Prevention and Data Recovery Planning.