

Emergence of Business Continuity to Ensure Business and IT Operations

Solutions to successfully meet the requirements of business continuity.

- 2 Introduction
- 3 Use of Virtualization Technology as a Business Continuity Tool
- 4 Challenges of Managing Virtualization Infrastructures
- 5 Maintaining Your Business Continuity Advantage

Introduction

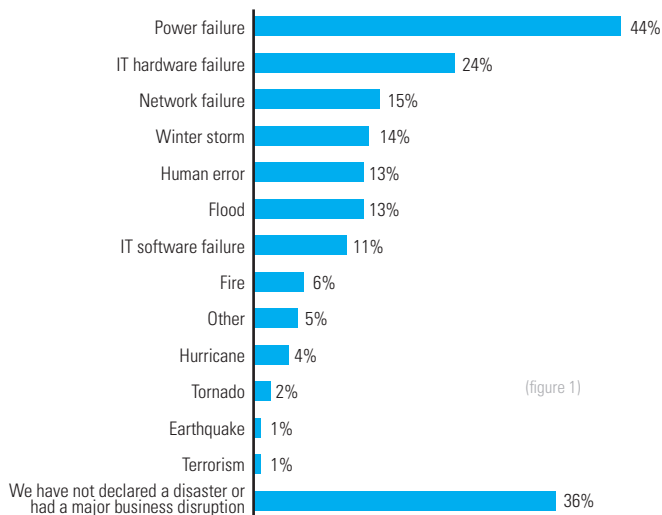
Over the past two decades, the practice of ensuring business continuity has matured as a business requirement within the corporate environment. In the early 90s, business continuity was conceived as a solution to protect mainframe computer systems and early data centers during a potential crisis or full-blown disaster. Business continuity was originally called “disaster recovery” and consisted of project planning and support from equipment vendors. As the profession developed, disaster recovery planning became a subset of an organization’s business continuity plan. The business continuity plan is now a comprehensive corporate policy that ensures that all of a business’ departments can successfully operate with minimal or limited impact during a disruptive event¹. Thus, a disaster recovery plan and emergency response procedures are part of the larger business continuity plan. What started as a formal procedure to protect expensive computer equipment has crossed over to protect all elements of a business organization.

An unrelated development, virtualization technology, or software that emulates computer hardware, has enabled the IT industry to consolidate data centers, revolutionizing the IT industry. These two developments, business continuity and virtualization technology, have increased IT operational efficiency and helped corporations meet business continuity objectives. Organizations benefit due to reductions in cost and increased protection of critical IT computer systems and data assets.

According to Forrester Research’s report on the business state of disaster recovery preparedness, a joint effort with the *Disaster Recovery Journal*², many organizations have improved their disaster recovery capabilities over the past few years. Despite a slow economy, survey respondents reported an increased confidence in being prepared for a data center disaster or site failure. It is noteworthy that the top causes of declared disasters or business disruption events include: power failure, IT hardware failure, natural disaster, and human error (see Figure 1). These common events have plagued information technology for years.

The business continuity plan is now a comprehensive corporate policy that ensures that all of a business’ departments can successfully operate with minimal or limited impact during a disruptive event.¹

“What was the cause(s) of your most significant disaster declaration(s) or major business disruption?”



Base: 200 disaster recovery decision makers and influencers at business globally (multiple responses accepted)
Source: Forrester/Disaster Recovery Journal November 2010 Global Disaster Recovery Preparedness Online Survey

¹ For purposes of this article a business disruption is anything that prevents day-to-day work from being done, including power disruption, downed phone lines, and so forth. A data disaster occurs when data is corrupted. Hence, a data disaster is a subset of business disruption.

² Forrester Research’s 2010 report on the business state of disaster recovery preparedness, a joint effort with the *Disaster Recovery Journal*: http://www.drj.com/images/surveys_pdf/forrester/2011Forrester_survey.pdf

Forty-seven percent of survey respondents acknowledged that they had calculated the cost of critical system downtime. This is a difficult cost to analyze because it takes into consideration not only productivity losses, missed sales opportunities, and staff's hourly time, but also less quantifiable impacts to downtime such as damage to corporate image and customer confidence. Yet according to the survey, only 15 percent of respondents could actually put a number to the cost of downtime; it averaged nearly \$145,000 USD per hour. A staggering cost indeed.

Adam Sills, vice president of errors and omissions with Allied World U.S., a reinsurance company that provides specific technology-based insurance policies, reports that there is a growing need for additional protection against business interruptions. The costs of a business interruption, whether due to network attack, data breach, or natural disaster, "can be a rude awakening for an organization," says Sills. The additional expense of researching the root causes and damage impact can be more than what traditional business insurance covers. As such, Sills reports that many of his clients have purchased technology insurance policies to mitigate risks presented by business interruption.

Most companies, according to Stewart, will purchase an in-depth risk assessment and then do nothing about it.

Staying prepared requires more than having a documented business continuity plan; it requires teamwork from all stakeholders. Having a stake helps to ensure that business operations will be maintained in the event of a disruption. Unfortunately, "many plans are written for auditors," says Don Stewart, director of professional services at Ongoing Operations, a non-profit business continuity service provider for U.S. credit unions. "Plans written at the last minute because an auditor will be arriving onsite—that cycle needs to be broken," Stewart says, and he recommends that a good plan starts with a risk impact analysis. Most companies, according to Stewart, will purchase an in-depth risk assessment and then do nothing about it. "The report just sits there with no further actions being taken."

Organizations must continually improve their business continuity and disaster recovery plans. The advent of virtualization technology has enabled more organizations to protect their business operations.

Use of Virtualization Technology as a Business Continuity Tool

Business continuity and IT do not always respond to business needs in tandem, it often is more of a struggle. The redundancy requirements that a business unit has for a new project can force compromises that put projects at risk. For example, an IT manager of a large private service corporation relates how just a few years ago, business leaders would be shocked at the estimates for computer systems. Senior management has "high expectations for resiliency and data redundancy and that would double or quadruple the equipment costs," this IT manager says. Then business leaders would re-evaluate their redundancy requirements and in the end, cost concerns would win out. IT staff and resources to manage these redundancy platforms, as well as the overall impact to the complexity of the IT infrastructure itself are additional costs under-appreciated by business leaders. Too often, business continuity takes a lower priority during planning.

The redundancy requirements that a business unit has for a new project can force compromises that put projects at risk.

Before virtualization technology existed, an organization had difficulty in meeting recovery time and system availability requirements due to the procurement of physical computer systems. Increasingly, virtualization technology is deployed within an organization and redundant computer systems can be provisioned quickly. Recently, the IT department of the U.S. State of Ohio virtualized the data centers that provide governmental social services to residents with developmental disabilities. The goal of the project was to provide employees and external users access to service applications without any downtime and the ability to scale for future growth. This project supports 80,000 Ohio residents. *TechTarget* reported on the project³ and relates how the entire project took nine months of architecture planning, and before they began building the infrastructure, disaster recovery requirements were a top priority. By leveraging the experience and expertise of internal staff and by working with a qualified third-party IT service company from the beginning, this project was completed on time and currently supports 200 virtual machines. More than 90% of the department's servers have been virtualized, *TechTarget* reports. This project is an excellent example of how IT virtualization projects can work in harmony with business continuity objectives to deliver quality services.

On the other hand, having a virtual infrastructure plus a disaster recovery plan does not equal business continuity readiness. Don Stewart, quoted earlier, cautions that “business continuity” and “disaster recovery” have been blurred. Stewart explains that business continuity is the overall plan an organization has in order to maintain business operations from all departments. Disaster recovery is the plan that IT and facilities can implement to restore key services, enabling business operations. The business impact analysis, measured in economic costs of a disaster event or business disruption, is often what drives recovery time objectives, according to Stewart.

Having a virtual infrastructure plus a disaster recovery plan does not equal business continuity readiness.

Challenges of Managing Virtualization Infrastructures

A Gartner Report⁴ observed that an organization's IT processes that have been developed over time are generally not structured for the “speed and rapid change” that virtualization provides. The Report confirmed that many organizations have deployed virtualization technology quite extensively. The challenge is that management tools and processes have not kept up.

“More skill-sets are required to handle the complexities of a virtualized infrastructure,” says Hugh Smallwood, chief technology officer at Ongoing Operations. “SAN technology architecture, security for virtual networks, and interaction with the host server at a command-line level is required and there's a learning curve,” Smallwood explains.

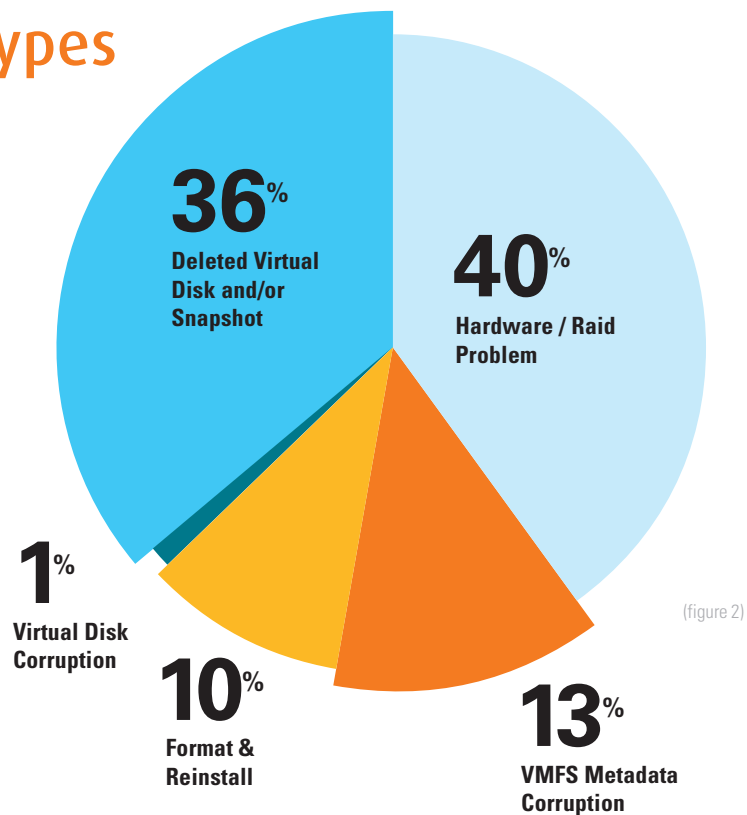
³ <http://searchservvirtualization.techtarget.com/news/1524700/Virtualization-should-start-with-disaster-recovery-says-Ohio-agency>

⁴ <http://www.vmware.com/files/pdf/analysts/Gartner-server-virtualization-leads-to-cloud-computing.pdf>

Maintaining Your Business Continuity Advantage

During the early days of business continuity's development, modern leaders realized that methods had to be developed to not only protect the immense investment in computer hardware systems, but to develop procedures for recovering these systems to a pre-disaster state. In fact, Kroll Ontrack, the leading provider in data recovery services, has seen a steady increase in the demand for recoveries from virtual systems. In 2010 the leading cause of VMware data loss failure was hardware/raid problems:

VMware® Data Loss Failure Types



Choosing a data recovery service vendor before a disaster occurs prepares the IT team for a successful survival of a business disruption.

As discussed, some organizations have enhanced their business continuity plans with additional insurance protection to cover the costs of data breaches or technological failures. Other organizations extensively architect disaster recovery procedures within their projects to protect their investments. One thing is for certain, it is vitally important to include data recovery processes within a corporation's business continuity plan. Successful organizations realize that any disruption, regardless of how small, will have an impact on the business as a whole. This has led IT leaders and business continuity planners to proactively include data recovery services in their contingency plans. Choosing a data recovery service vendor before a disaster occurs prepares the IT team for a successful survival of a business disruption.





For more information, call or visit us online.

800.872.2599 in the U.S. and Canada

+1.952.937.5161

www.krollontrack.com

Copyright © 2011 Kroll Ontrack Inc. All Rights Reserved.
Kroll Ontrack, Ontrack and other Kroll Ontrack brand and product names referred to herein are trademarks or registered trademarks of Kroll Ontrack Inc. and/or its parent company, Kroll Inc., in the United States and/or other countries. All other brand and product names are trademarks or registered trademarks of their respective owners.