

Enterprise, Know Thyself!

BC/DR in Business Context

By Michael Croy, Forsythe

The day-to-day pressure on business and IT leaders to optimize and secure their IT for performance and profit is enormous. Add to this the complication of meeting compliance regulations. In the face of these needs, getting an organization to focus on and fund business continuity and disaster recovery (BC/DR) planning and infrastructure continues to be a great challenge.

By placing BC/DR considerations firmly within the business context of IT, seeming contradictions are erased. The same infrastructure that ensures *resilience* and affordable *recoverability* in the face of crisis, improves performance and profitability today. Investment is still required, but the payoff is immediate.

Understanding the Business Context of Your IT

The business context of your IT is the “shape” of your business. It is a unique identifier for every organization. Many businesses in the economy share a basic business identity with others—they sell shoes, make umbrellas, deliver financial services, etc. However, each organization’s infrastructure is unique, having grown one piece here, one piece there, as the business’s needs have expanded and evolved. Each encompasses a particular arrangement of technologies and runs a different group of applications. The technology infrastructure side: network, storage, server, security, and facilities; and the business side: functions, processes, and applications; are intended to drive performance and profitability day-to-day. The unique business context is the sum total of specific functions and interdependencies that meet the organization’s objectives, encompassing all the elements of the company’s human, business, and technical infrastructure.

In addition, even within the same industry, every organization defines its business objectives a bit differently. And each organization is driven by a specific set of fiscal and fiduciary responsibilities. On the fiscal side, profit expectations vary and are measured differently from business to business. Cash flow and its handling varies. Bank covenants have different impacts. On the fiduciary side, privately-held businesses don’t face the same federal

and state regulations as public companies do. Corporate governance requirements, industry regulations, audit requirements, customer and partner service level agreements (SLAs), and quality of service (QoS) requirements impact different organizations in different ways. Combined, each set of drivers creates a unique daily business paradigm which determines how much investment is available and required to support each part of the paradigm.

“Enlightened” Risk Management

True risk management requires an intimate understanding of what is needed to sustain the business. Risk management decisions can be broken down very simply into three categories.

An organization can choose to accept a vulnerability or risk—maybe the chances of it happening are very slim, or the cost of the impact to the organization is small (enough). *Or, the risk can be assigned*—either by insuring it or by outsourcing it. Outsourcing could mean bringing in other specialty organizations to help support the business in specific areas, such as the human resources or payroll functions, or the entire IT organization. The third possibility is to *mitigate the risk* to some appropriate level. The goal is to reduce the risk, in terms of dollars and cents, to a risk that is acceptable (affordable) to the organization. Some organizations will determine that they need to spend a billion dollars to adequately reduce their risk. Some organizations will spend a hundred dollars. Determining how much to spend and how to spend it is where the introspection comes in.

Part of the mitigation decision is whether to mitigate the risk proactively or reactively. A trading floor that cannot go down may invest in a synchronous replicated site to back up data and maintain availability to the keystroke. It will have personnel at multiple locations to enable instantaneous cutover of operations in the event of a business interruption. Another organization may determine that, on balance, it can manage with a 24-48 hour recovery window. It may have a plan for personnel relocation or dispersal only in the event of a crisis.

Achieving Enlightenment or Closing the Business Continuity Gap

The “business continuity gap” refers to the difference between what the business needs at time of crisis and the reality of what IT can provide in terms of information availability and business functionality at time of crisis. It takes a great deal of corporate and business unit planning and IT investment to close the gap so that investment and risk decisions can be made based on accurate information and realistic expectations. The key, again, is arriving at an intimate understanding of what is truly needed to sustain the business—and what is possible to achieve.

Take the example of a unionized energy company. Its greatest area of exposure in the event of a systems outage was, in fact, not its productivity, but its payroll. Operations could be maintained with limited systems availability, but if it ever failed to produce paychecks, *it could be fined many, many dollars by the state and the union might call its workforce to strike.*

Once this was understood, its business continuity plan became focused on how to handle payroll. The decision was made to outsource its payroll processing to a major, national payroll services company. The payroll service had already made a substantial investment to keep its payroll infrastructure up and running without interruption. *This made sense because payroll services are its core business,* whereas payroll was not the primary business competency of the energy company.

The energy company went a crucial step further. It negotiated an agreement with the union that, if its systems went down and were unable to calculate a given week’s actual paychecks, paychecks would be issued in amounts reflecting the last available week’s information. By doing so, the company extended its recovery time and recovery point objectives by at least a week, greatly lowering the cost of its BC/DR infrastructure investment *while ensuring that an interruption in its payroll information would not result in extensive fines and shut down its operations.* This plan required the company to truly understand its mission-critical needs. Many enterprises have yet to achieve this level of self-knowledge.

The Next Plateau—From Being Prepared to Leveraging Your Preparedness

At the end of the day, the fundamental obstacle to true business continuity and disaster recovery preparedness is cost. Or, to put it more accurately, perceived cost. As discussed earlier, actual cost must be balanced against the costs and damage caused by failure to prepare adequately to support a given business context. But while BC/DR investment was once viewed as a black hole, today it is an investment that provides immediate rewards.

One reason this happens is that the same technologies and increased enterprise awareness that enable effective, cost-efficient business continuity also optimize day-to-day IT support of business functions.

Server virtualization not only increases BC/DR capability and flexibility by allowing restoration of any “system” on another virtualized infrastructure, but also increases overall physical platform resource utilization and helps control data center power and cooling constraints. It enables new systems to be provisioned from existing infrastructure rather than purchasing additional physical platforms. It enables better alignment of applications and balancing of workloads on existing resources. And it enables maintenance to be performed without downtime to critical application environments.

IP networks not only increase BC/DR capabilities and resiliency, but also reduce capital and operational expenses—especially in the area of change management—and optimize work flows. The related technologies of VoIP, unified messaging and integrated conferencing improve communications capabilities and enable more efficient, less costly storage, backup, recovery, and archiving.

Information management policies and technologies such as tiered storage and storage resource management enable organizations to more easily meet storage, security and privacy compliance requirements. At the same time, they reduce the cost of information recovery by categorizing and prioritizing recovery needs.

Another immediate reward of BC/DR is competitive advantage. As more organizations establish interdependencies with their customers, partners, and suppliers—whether through actual information flows or service level agreements firms are increasingly considering the business continuity profile of potential partners and suppliers when deciding where to spend their money. It stands to reason, then, that an organization’s BC/DR preparedness is becoming an important differentiator, which can be marketed as a competitive advantage.

This new reality brings us full circle to the inevitable relationship between resiliency and recoverability, and performance and profitability. Enterprises that can see the connection and use their self-knowledge to invest accordingly are the enterprises that will endure not only at time of crisis, but in the day-to-day marketplace. When viewed from this perspective, it becomes clear that solid business continuity and disaster recovery plans based upon the unique business context of an organization’s IT are not only good investments, but good investment protection.

Published in Disaster Recovery Journal, April 25, 2007.

Also published in Forsythe Focus, Winter, 2007.

Michael Croy is Forsythe's director of business continuity solutions. With more than 20 years of experience, he is responsible for the company's business continuity offerings, including risk analysis, best practice models for continuity of IT infrastructure (storage, server, and network) and disaster recovery planning, strategy, and management.



800-843-4488 | www.forsythe.com

© 2007 Forsythe Solutions Group, Inc. All Rights Reserved. Contents may not be reproduced, in part or in whole, without prior written permission from Forsythe.