

# Business Continuity for IT Managers

By William Laurent

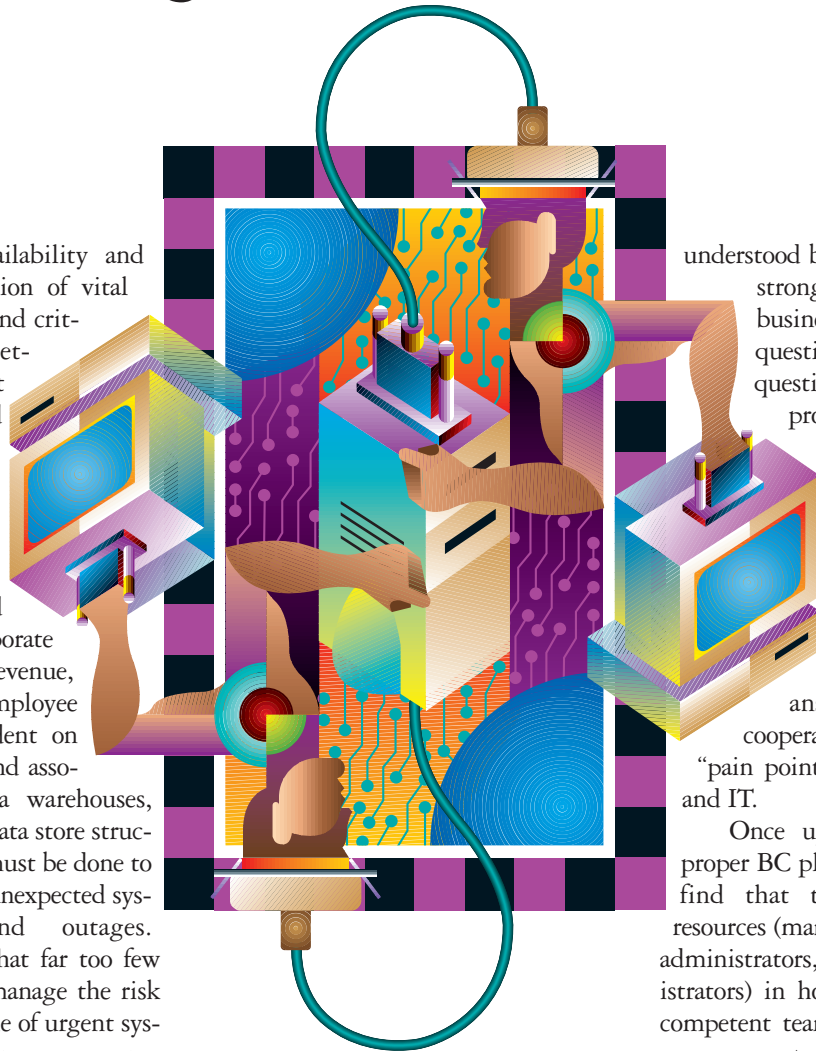
Ensuring total availability and continuous operation of vital business systems and critical data – bullet-proofing against potential failures related to disasters, crashes, sabotage, maintenance and other anomalies – tops the list of urgent considerations for today’s enterprises, large and small. When vital corporate concerns such as sales revenue, customer service and employee productivity are dependent on integral dynamic data and associated repositories (data warehouses, data marts, operational data store structures, etc.), the utmost must be done to prevent and respond to unexpected system degradation and outages. Experience has shown that far too few organizations properly manage the risk associated with downtime of urgent systems and warehouses. For many companies, it would take “days or longer” to recover lost or damaged enterprise data. This sort of time to recovery is unacceptable. Business continuity should be treated as *business survival*. Let us confront some of the issues associated with proper *business continuity* (BC) practices – expounding on both technology and business areas of interest.

A business continuity plan is meant to encompass the whole business – not just key network, database and application areas. It should not be limited in scope to information technology (IT) considerations! Remember that IT exists to fortify and enhance the multitude of

business operations that must be maintained in times of crisis. Technological decisions in support of continuous operations must not be made in a vacuum. In other words, IT continuity is a subset of BC. Business functions and IT functions must carefully collaborate and complement each other. Business continuity is a shared effort between business management and IT management, across departments and business lines, where all stakeholders must express and understand the criticality of data, systems, business process and the overall mission of BC. Only when the benefit and value of a BC effort is demonstrated to and

understood by executive sponsors and strongly aligned with overall business objectives can seminal questions be asked. “What-if” questions (about such things as projected lost revenue per hour in sales applications, minimum historical data required for customer service and field representatives to function, legal liability and so forth) cannot be effectively answered without close cooperation and identification of “pain points” between the business and IT.

Once upper-level buy-in for a proper BC plan is in place, companies find that they usually have the resources (managers, auditors, database administrators, network/system administrators) in house to quickly form an competent team; nevertheless, effective management of the information gathering, planning, auditing and plan dissemination process will be complex. From a perspective of technology alone, achieving continuity has become exponentially more complicated every year due to compliance issues, outsourced/off-shored data, Internet and n-tier architectures, and staff/resource issues, to name a few. Because of the diversified set of skills and extensive knowledge required to lead a large BC effort, somebody with past BC credentials (or similar) should manage putting this team together as well as the team itself. For example, you may have a former Y2K remediation



project leader that could smoothly transition into this role.

Departments can learn from one another – via structured cooperation and integrated JAD-type meetings – so that a comprehensive and effective *business impact analysis* can be performed. The impact analysis should list the firm’s prioritized business processes and take into account the interfaces with vendors, suppliers and third-party companies. In fact, many BC plans are brittle because not enough consideration is given to dependencies on third-party data feeds, delivery schedules, service agreements and more. Your BC chain may be only as good as the weakest link of your outside partner’s outfit; therefore, strongly demand that they familiarize you with such things as their continuity plans/programs and disaster recovery audit reports. Based on clearly defined, documented and recognized standards and risk ratings, this information should be easily understood by all interested parties and made freely available. Never forget that *a third-party data loss may be your data loss*, impacting everything from customer service to application development to data mart availability.

Once an integrated hierarchy of your systems and applications (in order of criticality) has been documented (taking inventory of various networks, resources, data, hardware, customers, business tasks, etc.), a prioritization plan for recovery and restoration of these interdependent components can be modeled. This plan should detail the order in which mission-critical items are to be rectified, as no two components will require equal protection or recovery time if risk is to be managed properly. Of course, you will have to make sure BC plan evaluations and updates occur on a semi-regular basis or when significant systems or business process change occurs. Your comprehensive plan (including downtime contingency plans, debriefing session logistics, recovery teams, insurance claims filing procedures and more) should be updated regularly and have an owner who is responsible for its maintenance and its quick, shared and safe access. Coordinated plan dissemination should happen at regular predetermined intervals so that BC becomes emblazoned on the organiza-

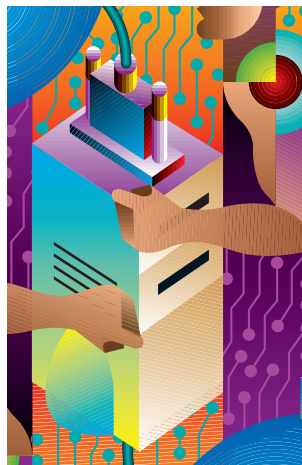
tion’s collective consciousness.

Often, BC arrangements are based on specific disaster scenarios and will not withstand unconsidered, yet realistic occurrences. Disasters do not follow a simple and focused prospectus; they are unpredictable, uncontrolled events. Preconsidered events may have little relationship to real-life circumstances or fundamental needs, lulling a company into a false sense of security with unqualified hunches about the availability and exposure of people, data, hardware and networks. Additionally, remember that most plans do not achieve a comfortable degree of success when first tested. What is more, many test scenarios are never traversed, even cursorily. Weaknesses are not exposed, endangering not only expedient and uncorrupted system recovery, but fundamental business core values. You must start by asking: Where (physically and logically) are we most vulnerable? Then, make sure that BC plans and implementations are defined and modeled within the manifest context of your unique industry or associated business line. (Best practices in BC may be drastically different for a finance company than for a food and produce company.)

More and more, business continuity has a global perspective. Typically, many companies have a complex web of geographically dispersed data centers, application users and customers. Data must be available, redundant and continuous across geographical areas (sometimes continents) and units of business. This heightens the possibility that a disaster or adverse events will “roll over” the enterprise, as storage devices, software or network connections shed continuous operation by unexpectedly failing independently – over a time span that could be minutes or days – resulting in corrupted and unusable data that is very difficult to identify and recover. Proper gatekeeping should isolate a rolling disaster so it does not propagate, while physical and logical access control at remote sites must be cleverly managed in order to quickly curb further

complications that may be poised to roll in. Speeding such recoveries depends on the intervention of humans that can obtain both logical and/or physical access to affected systems. Often, businesses lack formal communications plans to inform, contact and protect key recovery staff and business partners in the event of problems. The formation of an *emergency response team* (ERT), as well as protocols for team communication, should be part of any BC plan.

Aside from personnel and procedure issues, a good BC manager will understand the physical intricacies of repository storage infrastructure: the world of off-site storage and restoration, hot/cold/warm backups, recovery server farms, geographically scattered standby systems and beyond. Although too large to cover in detail in this article, an understanding of some basic and relevant infrastructure concepts is imperative.



To attain certifiable “just in time” system resumption and acceptable continuity of business operations, companies must have 24x7 ability to recover and restore their most recent working configurations of data, files and applications. Such endeavors begin by gaining platform integrity with an information storage infrastructure that will eradicate or greatly

reduce the peril of a single point of failure in the server, the network or storage mechanisms. A huge range of IT BC tactics exist (disk mirroring, clustered machine pairs, coordinated off-site disk or tape backups and techniques ad infinitum) that will help the enterprise secure critical and continuously available data, and give fault tolerance to applications and dependent business processes. (The traditional off-site tape-dump paradigm, while fine for batch systems, no longer satisfies most disaster recovery and challenging BC requirements for e-business, data warehouses and other dynamic IT complexes.)

For most chief information officers (CIOs), hardware redundancy is usually considered the primary means of defense


against incidents that would negatively impact the steadfast function of IT systems and the greater whole of the business. An arsenal of protection against the common foes of server, drive and disk failure is of primary importance. Voluminous processors in a single machine can offer protection from processor failures, while several machines in a cluster formation will insulate important systems from the adversity of machine failures. Drive redundancy can be achieved by using RAID (redundant array of independent disks) and disk mirroring solutions; RAID cabinets with extra storage and drives – in conjunction with a robust disk mirroring blueprint – will increase fault tolerance and farm out the strains of unplanned restarts, emergency recoveries and various continuity safeguarding burdens for very large system architectures. A system's overall performance must not be degraded in the event of hardware failures, thus a balanced RAID and redundancy architecture is imperative. Such a formation will also be a boon to connection transparency. Users that have accessed a failed component, database, feed or allied element should have no idea that it has gone down, as they are transparently – no disruptions detectable – switched over to another immediately available failover copy (and back to the original when it is brought on line). This transparency will be aided by logical replication practices, such as more frequent backup windows and database-centric validation before redundant copies are written to backup medium that will provide added data availability, improved data integrity and reduced recovery time.

Keep in mind that although most IT shops have procedures in place to implement a switchable (emergency cold standby) essential data copy, failover situations are usually anything but seamless. Even in the simplest of contexts, the overhead and resources of a second backup server that mimics the production database and applications will be utilized and, therefore, must be managed properly. In scrambling up the ladder of disaster or outage recovery, restoring a production database from this backup/remote server is often the final rung; unfortunately, many compa-

nies look at the front end of this scenario – backup performance – and not restoration performance. It is always quicker to back data up (usually subsets) than it is to fully restore an entire database, and organizations need to make sure that recovery and restoration time is tracked and benchmarked as part of a robust and airtight BC plan on the IT side. Yet, many businesses underestimate the time involved (and are thus surprised at vulnerable moments) in restoring data during a crisis – affecting everything from end users to executives, customers, suppliers, development teams and beyond.

Realizing a weatherproof replication strategy (the two primary types being synchronous and asynchronous replication) will ensure that your IT command is supporting companywide BC. *Synchronous replication* strategies guarantee that a primary site's mission-critical data is mirrored and backed up at a separate/remote location with a solid degree of consistency. Data will usually be updated or rolled back at shared commit points mutual to both locations, thus quantizing data integrity and consistency to a "last confirmed state." Properly implemented, this *two-phase replication* lends itself to synchronous, quick and consistent recovery of crucial data and applications. Nevertheless, latency problems may occur as propagation delays can exponentially lengthen with increased distances. Introducing distance limitations associated with synchronous replication may bode ill for quick recovery and failover if a remote site and its mirrored data still reside too close to the disaster or impact zone. In a similar vein, *asynchronous replication* lends itself to recovery processes that span much greater distances, usually using Internet Protocol (IP) networks where the primary host-data "write to storage" operation is disconnected from the remote write operation, reducing the high latency associated with tape backup methodologies. Businesses can write, store and recover data at remote sites that lie safely beyond a disruption's hot zone, sometimes thousands of miles away; however, data consistency issues may come to light because asynchronous replication does not always wait for airtight confirmation that a

principal write operation has completed/succeeded at the remote site before it continues with the next operation. The most solid approach will often combine elements of synchronous and asynchronous regimens in order to minimize data loss over very long distances while maintaining multisite integrity and consistency. This may commonly involve three or more data center, recovery/startup or mirroring sites – both onshore and offshore – that act as resynchronization, remote data queuing and remote pairing agents (although added cost and management complexity may increase quickly). However, special attention will have to be given to the associated networks – accept that they are vulnerable and devise continuity controls accordingly.

In these days of complicated e-business and international data warehouse architectures, throwing hardware at a system to ensure IT business continuity will not help. IT assets and business processes must be viewed as a symbiotic whole that depend on one another. Only by taking stock of systems' hierarchical importance, gauging risk, documenting and auditing all key components – logical and physical, business and technical, remote and local (third-party partners' data feeds, resource roles, customers dependencies and more) – will enterprises be able to effectively take steps to reduce costly fallout from downtime/degradation of mission-critical systems and data. The adroit BC expert will think beyond the basics of securing data in its raw low-level (set of vanilla data files) format and confront the substantive definition and value usage of the data and its interaction with applications, people and empirical business processes. 

---

William Laurent resides in New York City and is the executive vice president of Loyer TCG where he leads the company's newly founded Data Warehousing practice. Laurent has a diverse systems background, successfully designing and managing the implementation of projects for the insurance, banking, finance, publishing, government, technology, entertainment and hospitality industries. The author of several white papers, he continues to be in demand as a data warehouse architect and lecturer. Laurent would enjoy receiving your comments, ideas or inquiries via e-mail at [blaurent@loyertcg.com](mailto:blaurent@loyertcg.com).

