
Business Continuity and Disaster Recovery Planning: The Essentials for Any Business

Planning for business continuity and disaster recovery is one of the most fundamentally important preventive steps a business can take to ensure its own long-term survival.

Routine business operations can be interrupted by any number of unforeseen events—from weather disasters to pandemics to human error leading to a temporary or permanent loss of data. A significant business interruption can be catastrophic without solid advance planning, and recent events strongly suggest that certain types of disasters will become more common in the years ahead.

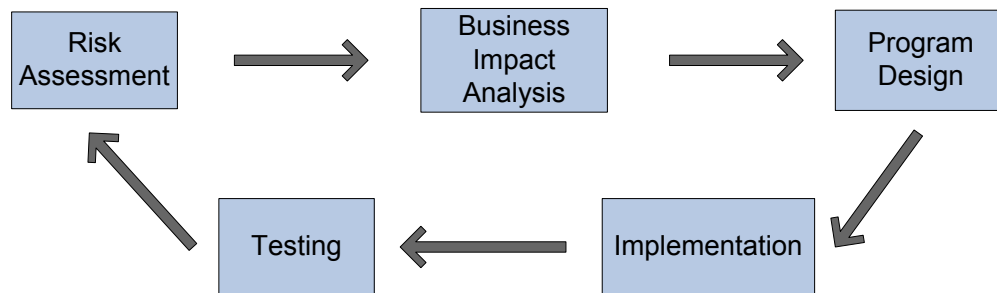
When the cost of catastrophic data loss can run as high as \$2,000 per minute,¹ it is troubling that business owners and senior managers fail to make the proactive investments in IT infrastructure and in-house systems and procedures that will protect their operations when—not if—disaster strikes. Organizations that do make a serious commitment to business continuity and disaster recovery planning reap the additional reward of more efficient, effective operations, since the systems behind a robust emergency plan also help streamline routine IT processes.

Definitions

The following definitions² are central to any discussion of business continuity and disaster recovery.

Business continuity

A business continuity plan evolves from a process that identifies mission-critical business processes and enacts procedures that enable continuous operation in the event of unforeseen adverse conditions. It is produced at the enterprise level and consists of a five-stage, continuous loop: from risk assessment, to business impact analysis, to program design, to implementation, to testing, back to the next round of risk assessment.

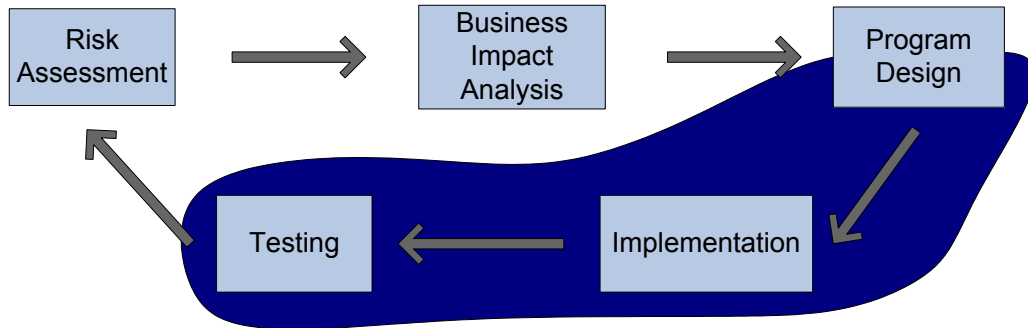


¹ Robertson, Kris and Mary Bennett, Tridex Systems Ltd., presentation to *TUG 2010 U2U*, April 23, 2010, Colorado Springs, CO.

² From Robertson and Bennett, *ibid.*

Disaster recovery

A disaster recovery plan sets the business continuity plan in motion by defining the procedures required to restore IT systems, applications, and data and provide access to user community. As the tactical expression of a strategic framework, it overlaps the operational elements of the business continuity plan.



Virtualization

By taking full advantage of the higher power of state-of-the-art CPU chips, virtualization allows users to consolidate IT operations from multiple mainframes and sites on a much smaller number of servers. During routine operations, virtualization improves efficiency and reduces costs. As a central element of a business continuity plan, virtualization simplifies and streamlines the process of recovering mission-critical data in the event of interruption or loss.

The Scope of the Issue

The causes of business interruption

A variety of factors can interrupt access to the critical data and IT systems on which successful business operations depend. Kris Robertson of Tridex Systems, Inc. listed a series of disaster scenarios during a presentation to TheUserGroup.org's TUG2010U2U conference in Colorado Springs, CO April 2010, including floods, hurricanes, plane crashes, and even the unexpected death of key personnel.

But although natural and physical disasters command the most attention, by far the largest share of business interruption related to IT infrastructure involves hardware malfunction, human error, software corruption, or viruses. Data backup provider Protect Data³ attributes the continuing rise in data loss to three factors:

³ www.protect-data.com/information/statistics.html

- More data being stored in smaller places (and, often, on tape media that become less reliable over time)
- Heavier reliance on mission-critical data
- Backup tools and, especially, backup procedures that are less than 100% reliable.

Robertson and co-presenter Mary Bennett cited Protect Data's finding that more than three-quarters of business interruptions result from hardware malfunctions and human error. Protect Data ranks the causes of data loss as follows:

- Hardware or system malfunction (44%)
- Human error (32%)
- Software corruption (14%)
- Computer viruses (7%)
- Natural disasters (3%)

Robertson described the disruption experienced by one Infor customer located near the site of a recent propane explosion. "While the event wasn't at their business, they saw a severe impact because they couldn't get their trucks in and out." Bennett recalled two customers who had contacted her in the previous two months. In one case, an IT manager working as a temporary replacement accidentally deleted a root directory, leading to a full day of down time before backups were fully installed. In the other, the IT team had failed to verify that their backup tapes actually contained usable data, and only realized the error when their Windows box crashed.

"It took a week to get that server back up and running. So human error happens, even to the best of us," Bennett said. "I want you to think about that: When was the last time you verified your tapes?" "It's been a while," a participant replied. "Then go home," she said. "You have your assignment."

The business impact

Robertson emphasized the steep cost of interrupting data or IT infrastructure access for a single day. For a \$25 million company that operates 250 days per year, an average business day is worth \$100,000. At a gross margin of 25% and net profit of 3%, that means a day of lost business costs \$25,000 in margin and \$3,000 in profit. In a week, those figures grow to \$125,000 and \$15,000, excluding lost productivity, overtime costs, and extra expenses.

Bennett said companies should have a clear idea of their "down time dollar number," the length of time they can afford to be offline before the business impact becomes severe. "That answer varies according to your ERP system, but it also involves Exchange, since the world runs on email now. Exchange, Blackberry, and iPhone have escalated to a critical part of your business." A participant recalled an internal audit revealing that his company's Exchange server was more

important than its enterprise system. “We can manage without SX for a while longer, but the second that Exchange server goes down, you know it.”

Beyond routine operations, Robertson said there are times and situations when businesses face significantly higher exposure. A cyclical business is more vulnerable during its busiest season. A company with a unique product operating in a niche market may be a bit more secure, but a firm with multiple competitors is more easily replaced. Data loss is critical when a business has to manage and move a large inventory quickly. And an organization may be subject to fines or lawsuits if an interruption prevents it from meeting contractual obligations.

For one customer that valued its down time at \$2,000 per minute, “there would be some serious ramifications to not having the system” for even a 24-hour interruption.

Speaking less than a week before the explosion on British Petroleum’s Deepwater Horizon drilling platform in the Gulf of Mexico, Robertson cited a study that tracked the impact of catastrophes, mostly man-made disasters, on the shareholder value of publicly traded companies.⁴ While the authors studied several companies that recovered fairly quickly from the market impacts that followed major disasters, those that did not had lost an average of almost 15% of shareholder value, a year after the events. (At time of writing, BP had lost 40% of shareholder value due to Deepwater Horizon.) Robertson noted that a crisis magnifies a company’s strengths and weaknesses, and while insurance will cover immediate losses, long-term success and survival depend on the ability to rapidly restore business operations.

For small businesses, the implications are even more striking. Of the companies that have no business continuity or disaster recovery plan when a catastrophe strikes, Robertson said 40% never reopen, 50% are out of business within two years, and 93% fail within five years.

“I would wager that just about all the attendees at this conference represent companies that are in that small business category,” he said, citing one area of the U.S. with high unemployment that had had flooding a couple of weeks before. “They were underwater, and there’s a really good chance that none of them will ever recover.”

Challenges on the horizon

Although the data on business interruption point to hardware, software, and human error as primary factors, Robertson’s observations on flood and weather damage point to an emerging body of knowledge on the changing character of emergency preparedness. From the devastating impact of Hurricanes Katrina and Rita in 2005, to deadly heat waves in North America and Europe, to record flash floods in Tennessee in May 2010, to shifting patterns of disease, businesses can expect increases in the number and severity of major events that may threaten operations, supply chains, and everyday commerce.

⁴ Knight, Rory F. and Deborah J. Pretty, *The Impact of Catastrophes on Shareholder Value*, Oxford Executive Research Briefings, undated, www.nrf.com/Attachments.asp?id=12546.

As two of the most authoritative U.S. sources on the magnitude and impact of an enhanced greenhouse effect, the Pew Center on Climate Change⁵ and the Climate Institute⁶ cite a series of outcomes of accelerating climate change, including:

- Sea level rise
- Increases in tropical storms and severe weather
- Heat waves
- Flooding in many communities, and drought in many others
- Resurgence of infectious diseases, including insect- and rodent-borne infections that will shift geographically in response to a warming climate
- Challenges to agriculture and food security
- Profound global security issues that have become a prime motivator behind climate legislation currently before the U.S. Senate.

Most if not all of the major outcomes of climate change bear directly or indirectly on the reliability and continuity of business operations. Over the last decade, climate change research and policy have proceeded along two parallel tracks: alongside the urgent effort to reduce greenhouse gas emissions, there is growing attention to the process of *adapting* to the inevitable effects of climate change. This intense focus reinforces the importance of effective business continuity measures that will prepare companies for a whole new category of threats.

A Five-Step Plan

Robertson and Bennett outlined the five components of a business continuity/disaster recovery plan:

- Risk assessment
- Business impact analysis
- Program design
- Implementation
- Testing

The first two stages focus on the “business continuity must-haves” that provide a cornerstone for effective planning. Robertson said an essential first step is to document the systems, processes, infrastructure, and supply chain relationships that a company needs to sustain and continue its operations. “All your critical business processes have to be documented, in hard copy and electronic form, in multiple locations, and with multiple people who know where to find the information,” he said.

⁵ http://www.pewclimate.org/global-warming-basics/facts_and_figures/impacts

⁶ <http://www.climate.org/topics/extreme-weather/index.html>

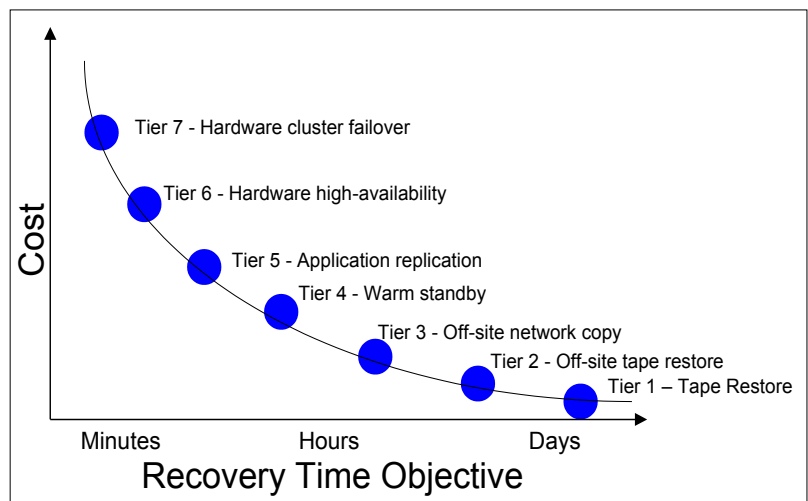
A complete risk assessment requires senior management to take a hard look at the company assets that would be jeopardized by a major disaster; business impact analysis involves quantifying the losses that would result. “Those two steps certainly involve the executives at the highest level of the company,” he said. The eventual program design “evolves from a process that identifies mission-critical business processes and enacts procedures that enable continuous operation in the event of unforeseen adverse conditions.” The full plan must eventually address everything from sourcing of office supplies to the ability to rely on insurance to replace lost inventory.

Bennett encouraged participants to talk to their senior decision-makers about the various key systems that support effective operations. Hardware and software (email servers as well as enterprise systems) are an obvious focus, but mundane components matter, too: she cited one client whose business continuity audit revealed that the phones weren’t even connected to a universal power supply.

“Some business owners would not care to have this discussion. Other business owners will embrace it. But you’ve got to get both types to embrace it,” she said. “They’ve got to face facts and at least understand: this is your business, these are the key areas, and you have to prioritize and make decisions.” The conversation may take more time and attention than businesses would prefer to devote in times of economic challenge, but “once you talk it through, at least you know what to do, and can start making the investments that are appropriate. You’re working on a plan, even if you don’t have all the pieces in place. What really hurts is if you haven’t had the discussion.”

Program design, implementation, and testing are the steps in the disaster recovery planning process that involve the IT department, and Robertson stressed the importance of continually updating the plan. “Everything you add after the plan is in place will have to consider the business continuity aspect as you deploy,” he said. “If you change businesses, if you sell off business lines or acquire new ones, that plan is a closed loop. But once you add or subtract things, the plan changes, and so do the systems.” Bennett urged participants to schedule quarterly reviews, to ensure that the business continuity updates actually take place. The focus on frequent reviews and updates was consistent with practices in sectors as varied as hospitality and public health, where emergency plans are subject to regular review, revision, and simulation exercises.

Robertson and Bennett said the recovery-time objective behind a business continuity plan is very much a matter of balancing speed



against cost. They presented a seven-point continuum of recovery strategies, ranging from a simple tape backup system to sophisticated, proprietary systems that offer the quickest recovery and highest level of fault tolerance.

The Value of Virtualization

Virtualization opens the door to massive reductions in server footprints and costs by drastically reducing hardware requirements and optimizing the use of disk space, RAM, and CPU capacity, Steve Owsley of Tridex Systems, Inc. told the recent TUG conference.

Owsley recalled one customer for whom Tridex virtualized 32 servers, reducing 25 physical boxes to two. Mainframes have been partitioned and subdivided for decades, but virtualization became an option for servers with the introduction of CPU chips so powerful that it was hard to justify buying new units that would largely go unused.

“You’re taking advantage of what’s idle on that server and making it available for one or more additional servers,” he said. “With fewer servers, you have lower operating costs.”

Virtualization simplifies remote access and control, and makes server rollouts and upgrades far more efficient. With a system like VMware virtualization software in place, “the server isn’t tied to the hardware anymore, so you can roll out new hardware really simply,” in a process that “takes minutes now, instead of hours or days,” Owsley said.

System administration time is reduced with only one piece of hardware to deal with, and VMware reports that virtualization reduces capital costs by up to 60%. Fewer servers mean less cost, less real estate, fewer racks, and drastic reductions in the cooling requirements that are standard for data centers. One Tridex customer who ran air conditioning all year round was able to shut it down during the winter of 2009-2010 after virtualizing her servers.

Virtualization is also an effective strategy for streamlining the system backups that are one of the cornerstones of a business continuity strategy. “Your rollout is basically however long it takes your infrastructure to complete that duplication,” Owsley said. The approach essentially eliminates system down time during routine maintenance, since server files can be migrated from one physical system to another without interruption.

In an emergency, installing the backup files and bringing them online is much more efficient in a virtualized environment. “Once you’ve put a server into a set of files, those files can be started anywhere and run somewhere else,” he explained. “Now you have a lot more flexibility. If you lose your hardware, you can bring the server up on another piece of hardware in minutes,” through either a cold or live migration.

How Tridex Addresses Business Continuity

As a leading global provider of application delivery and secure remote access solutions for terminal services and virtual desktop infrastructures, Tridex Systems, Inc. encourages its customers to take a proactive approach to business continuity and disaster recovery planning.

The company supplies a range of system backup applications and devices, offers advisory services for customers who are still coming to grips with their business continuity requirements, and provides installation and configuration services after backup systems have been acquired.

Tridex Systems is an innovative systems integration company founded in 1998 and headquartered in Colorado Springs, Colorado, with a second office in Englewood, Colorado. The firm prides itself in providing quality products and services to meet customers' needs. Over the years, Tridex Systems has expanded to encompass three areas of expertise: Business intelligence, managed services (including IT infrastructure), and thin-client enabling solutions. Tridex Systems provides everything an organization needs to set up and maintain a business continuity plan, including hosted solutions.

For further information on business continuity and disaster recovery planning, or on Tridex products and services, please contact:

Mary Bennett
Director, Managed Services
(303) 551-6471
maryb@tridexsys.com

Tim Watson
President
(303) 925-1375
timw@tridexsystems.com