Business Continuity for Global Enterprises: The Importance of Protecting and Managing Information Assets

MIKE RUETTGERS

INTRODUCTION

Global organizations are networks of online information flows. Very much like interrupting the flow of oxygen to the brain, when the flow of information into, through, and out of an organization is interrupted, key activities come to a stop. If the interruption lasts, the organism may die. Consider the cases of a multinational bank whose ATM network is not working, or an international airline that cannot access its reservation systems, or a worldwide brokerage whose e-mail system is down. In each of these cases, a business's inability to access its core of information and knowledge puts its revenues and its customer relationships at risk. Today, an ever-increasing amount of information lives inside intelligent data storage systems. One of the business contingency planning lessons of 9/11 is that simply backing up information is not enough to ensure its safety.[1] Disasters can be regional in scope, incapacitating both primary and backup facilities. For global organizations to build real resilience into their operations so they can continue to function no matter what kind of disaster strikes, they will need to keep copies of their most vital information in multiple locations on different combinations of hardware and software. This is the essence of business continuity.

Mike Ruettgers is Executive Chairman of EMC Corporation, a world leader in information storage systems, software, networks, and services. This article is adapted from his John R. Galvin International Leadership and Organizational Management Lecture, delivered at The Fletcher School of Law and Diplomacy in November 2002.

The catastrophic event of 9/11 spurred the executive offices of large organizations to reassess what needs protecting—people first, of course, then facilities and information—and how best to protect them. It broadened people's thinking from disaster recovery (or how long it takes a company to get back online after a disaster) to business continuity, a proactive approach to keeping critical business information and operations 100 percent available, regardless of planned or unplanned interruptions.

Business continuity equals revenue continuity. One hundred percent availability is the new standard in today's always-on business world. Customers and employees of global firms expect these businesses to be open around the clock and to operate with the reliability of dial tone. Business continuity is not just an information technology responsibility; rather, it is a business responsibility that requires involvement from boards of directors. But the corporate track record of progressing from an understanding of what needs to be done to actually investing the time, energy, and dollars to establish business continuity planning across the organization remains spotty. And that is a source of vulnerability, not only for individual companies, but also for the economy as a whole.

Business continuity equals one hundred percent availability in today's always-on business world.

This article will review several of the key business continuity lessons learned from September 11. It will present a framework for effective business continuity planning and advocate the need for linking business continuity to corporate governance so that good corporate governance will institutionalize business continuity.

BUSINESS CONTINUITY: LESSONS LEARNED FROM SEPTEMBER 11

Crises often bring clarity about what is truly important. In this post-9/11 world, there has been a sea change in the way large organizations prepare for disasters, think about, and care for their information. Here are six lessons learned from September 11:

1. All disasters are possible. Assume the worst. Plan for the impact of an outage. Companies in Florida tend to plan for hurricanes and power outages, companies in California plan for earthquakes, and in the Midwest they worry about tornadoes. September 11 made painfully clear that any kind of disaster is possible, anywhere. Hence, it may be smarter not to plan for a particular kind of outage, but rather to plan for the impact of an outage.

Narrowing planning to a single outage scenario and spending money to counteract an event of high probability may blindside a company to events of lower probability. It is far better to have the capability to contend with the worst

possible disruption imaginable by engineering resiliency into all aspects of a business's day-to-day operations.

2. Digital information is at the center of every business and most of its applications are critical. Global businesses now operate 24x7x365—always open, never closed. They understand that to operate "24xforever" they must have uninterrupted access to most—if not all—of their data streams and applications. E-mail, web access, payroll, billing, patient records, enterprise resource planning (ERP), customer relationship management (CRM), and supply chain management applications all need the highest levels of availability and therefore the highest levels of protection. For example, after the Twin Towers fell, a number of businesses in the vicinity found that their proposals in process, agreements for deals, and their ability to document transactions all existed solely in the form of e-mails. We used to think that only traditional revenue-producing transactions like processing customers' orders or shipping products mattered. On 9/11, we learned that e-mail had become equally important.

Not only is shared information indispensable to business, both as the glue holding enterprises together and the raw material for creating new products and services, but its volume continues to double each year. In fact, the size of the average data center is expected to grow from about 30 terabytes (tera is a trillion bytes, or all of the X-rays in a large hospital) in 2000 to more than 6,000 terabytes in 2010.[2] Managing, sharing, and protecting this information—and doing so cost effectively—is one of the toughest challenges facing companies around the world today.

According to the research firm IDC, many companies have already set goals of 99.999 percent availability for their critical enterprise applications.[3] "Five nines" means applications must be available for all but a few minutes each year. Achieving such high levels of availability may seem to be a hurdle that is difficult to clear, but companies may risk up to $6.5 million per hour when their applications are not available.[4] What is more, GartnerGroup Dataquest, an Information Technology (IT) research and consulting firm, estimates that two out of five companies that experienced an information-related disaster go out of business within five years.[5] Hence, maintaining uninterrupted access to digital information is vital to the survival of global businesses.

3. The distance between primary and secondary data centers matters. Two copies of data are not enough. Attempting to recover at a backup data center a few short blocks away or even one several miles away no longer makes sense. Disasters can be regional in scope, knocking out both primary and backup facilities—or, at the very least, the transportation infrastructures and power grids they share. That is why more companies are now locating their backup data centers a significant distance from their primary site. But disasters can go on for days, even weeks. When business processes suddenly became dependent on a single facility, even those companies with a second, distant site found themselves functioning well

below their set policy levels for protection and business continuity. The need now is clear for more than two copies of data and more than two dispersed sites for a company's crucial data. And global companies would be wise to create a third site on a different continent.

4. Inconsistent backup is no backup at all. Tape as a medium of recovery is not effective. Historically, standard disaster recovery methods have focused on the ability to copy data onto tapes, catalog the tapes, and then archive them in the event they are needed. But with the generation of new data far outpacing improvements in tape copy speed, recovery times from tape are far too slow. Tapes must be physically retrieved, transported, and loaded into tape drives for manual restores. Furthermore, it could take 10 hours to recover a single terabyte of data from tape and as much as a year or more to recover one petabyte (or 1,000 terabytes). And that assumes the tapes have not degraded. It takes only a few bits of compromised data to impede the process or even make full recovery impossible. What is more, tape-based information protection is unable to record events or transactions after the last completed backup. If a company backs up its data to tape only once every 24 hours, then it has the potential to lose up to 24 hours of transactions that cannot be recreated.

5. People-dependent processes do not suffice. There is a new mandate for automation. In any disaster, let alone one of September 11's magnitude, people think first of themselves and their families—and rightly so. And even when they are ready to turn to the work at hand, the ability to move them and their equipment and tapes to a recovery site may be impossible if, for example, that site is under martial law or quarantined because of chemical or biological contamination. In fact, the fallout from September 11 closed many streets, bridges, tunnels, and all airports. As a result, IT departments were unable to transfer their recovery personnel to their backup facilities. In addition, fatigued or worried employees can become error-prone, creating mistakes that extend the recovery process. The IT systems that performed best after the Twin Towers fell were those that could automate the task of recovery and limit the need for human intervention.

6. Outsourcing disaster recovery can create business risks. Many small- and medium-sized businesses rely on commercial records management and "hot site" providers[6] to hold duplicates of their data or provide a backup recovery site. These providers are an important part of business continuity implementations. But as a business expands and its information under management grows from tens to hundreds of terabytes, it should consider establishing its own business continuity infrastructure. Providers of outsourced disaster recovery services plan for only a modest percentage of their customers to require services simultaneously. In a large-scale disaster, there may be a sudden surge of competition for backup space by those firms that have contracted with an outsourcer, and consequently not enough capacity to go around.

DEVELOPING A FRAMEWORK FOR BUSINESS CONTINUITY

If those are the key lessons learned from September 11, what should global organizations do to build business continuity in its aftermath? The key is to engineer business continuity into the day-to-day operations of a business. That calls for three changes to an organization's information infrastructure.

First, businesses should consolidate storage and server devices so that all users can share from a common and protected information pool. Second, they should network their storage systems so no matter where the information resides—whether across the hall or across the globe—it can be accessed reliably and rapidly. This is done by placing networking devices between their storage systems and their servers, thereby giving them a central pool of storage to draw on and creating a single infrastructure that connects to all of their computing environments simultaneously. Third, advanced software should be used to automate the management of the entire infrastructure. When businesses consolidate their information, they find it far easier to manage, control, and synchronize these essential assets. This makes it easier to protect information, automate backups and instant restores, and guarantee the safety of information both locally and over long distances. Consider what happens when organizations rely on individual PC users to back up their own data. A 2002 research conducted by SRC indicates that up to 92 percent of all business PCs are not being backed up at all.

Business continuity is not a switch that can be flicked on. Instead, it is a capability that firms must build in stages.

Business continuity is not a switch that can be flicked on. Instead, it is a capability that firms must build in stages—six stages for maximum information availability and business continuity. The first stage should eliminate any single point of failure in the server, switch, or storage. The second stage should ensure that a business can back up its data frequently, consistently, and without disruption. The third stage should ensure that a business can recover its data quickly, accurately, and with predictable results. These first three stages—platform, backup, and recovery integrity—define protection within the data center.

Stages four through six should extend protection to a remote site since all data centers are vulnerable. The fourth stage should place a copy of all critical data at a remote site and ensure its availability for immediate use. The fifth stage should achieve remote processing integrity by integrating processors at the recovery site and creating an automatic fail-over[7] and resumption capability. The sixth and final stage would integrate multiple sites so that workloads can be moved from one location to other distant locations. Doing so will deliver the multiple

redundancies required in the most aggressively regulated industries such as financial services. A major distinction that must be made in the six-step continuum is whether or not geographical separation of a corporation's data centers is required. Increasingly the answer is "yes." Without this physical separation, the implication is that a company can afford to (or is willing to) lose 24-48 hours of transaction data. Therefore, before attacking the six-step process, it is important to establish the relative value of a company's information, frequently achieved through a Business Impact Analysis (BIA).

Undertaking a BIA process (or its equivalent) is critical in establishing a company's Recovery Time Objective (i.e., maximum tolerable downtime) and Recovery Point Objective (maximum allowable lost data). BIA's should clearly define Recovery Time Objective (RTO) and Recovery Point Objective (RPO). Generally speaking, if both RTO and RPO exceed 48 hours, focusing on the first three steps may be adequate. If either is under 48 hours, it is probably necessary to consider geographic projection of business transactions to an alternate facility and storage devices. Of course, not every company will need to progress through all six stages. But every company will need the ability to increase the level of protection as its business grows.

Building continuity and resiliency into a business demands the coordination and involvement of senior management and nearly every department within an organization as well as its entire value chain—customers, partners, and suppliers.

Companies need to understand and be able to quantify the cost of downtime and the cost of losing transactions outright in their business. They also need to understand their current ability to protect those transactions from interruption. For example, a survey conducted by InformationWeek Research found that nearly 40 percent of all companies surveyed say it will take days or longer to bring records back online if disaster wipes out their companies' main data stores.[8] That is significant economic loss.

With the information gathered internally within a business among its operating groups, the focus should turn to the business continuity strategy plan itself—how best to address each mission-critical business process.

Let us review how this approach worked in practice for two global financial services firms. Only days before the September 11, 2001 terrorist attacks, Commerzbank, the world's 16th largest bank, handling $30 billion in transactions daily, implemented a business continuity plan for its New York City offices. Their offices, on the 33rd floor of Two World Financial Center, only 300 feet from the World Trade Center towers, lost hundreds of windows and were covered in debris. When the World Trade Center crumbled, Commerzbank was able to immediately secure its customer transactions, financial databases, e-mail, and other critical applications by using a combination of networked storage platforms and automated software that replicated its core data to a remote site, creating an

immediately functional environment in which to carry on with business.[9] According to Gene Batan, Commerzbank's vice president of Information Technology Systems for North America, before the bank deployed this new technology, it was relying on tape for backup and restoration. "In the event of a disaster, the integrity of our information was at the mercy of the last time we backed up to tape, and restoration time would take at least a few days."[10] While it took Wall Street nearly a week to resume trading, Commerzbank's information was ready for business in hours, even before the company's employees could reassemble at a disaster recovery site 30 miles away in Rye, New York.

Other global financial service companies have adopted comparable approaches to comprehensive business continuity planning. For MasterCard International, which manages as many as 32 million transactions a day in 210 countries, information protection and continuous availability are at the core of its entire business strategy. "We don't sell widgets. We sell transactions. So if customers can't make transactions, it's a problem for them, for our members, and for us," says Brian Lock, MasterCard International's vice president for technology and architecture services.[11] MasterCard has a dedicated inter-departmental team that prepares for any contingency and finds ways to manage it. "As the demand for information grows, we have to move it from our network server to our data warehouse to make it usable. Information infrastructure isn't supporting our business—it is our business," notes Brian Lock.[12] The company has been perfecting its business continuity plan since 1990 and tests it twice each year by shifting its critical workload to backup operations and conducting comprehensive continuity exercises.

BUSINESS CONTINUITY AND CORPORATE GOVERNANCE

Good corporate governance cannot be separated from leadership evidenced over the long haul. That means that governance and continuity are intertwined. Reviewing and approving a workable business continuity plan is an important part of a corporate board's duty.

"The first thing that a board should do is to realize that information is one of the company's most important assets," says Tom Horton, a former chairman of the National Association of Corporate Directors (NACD), who currently chairs the NACD's Information Security Panel. "And along with that goes your reputation, which is hard to put a price tag on," he says. "Boards of directors aren't supposed to know all about electronic cookies and bots and firewalls, but they are responsible for the health of their company in perpetuity."[13]

In the wake of the September 11 attacks, directors of global companies have been reminded that they, too, are responsible for overseeing the creation of comprehensive contingency plans that are detailed enough to keep myriad functions operational, yet broad and flexible enough to cover many types of emergencies.

Corporate governance experts and regulators agree that, at a minimum, the board should review existing plans once a year, preferably delegating the job to the audit committee. The board also should require that the business continuity plans be tested and be evaluated for performance after any emergency that requires its implementation.

Specifically, corporate boards should direct four key questions to their corporate officers.

1. How long would it take to recover the business if we have a disaster? If it takes more than 24 hours to get core business functions back up, that is too long. This critical measure of preparedness is frequently in excess of 48 hours for organizations that rely on tape backups.

In the wake of September 11, global corporate leadership today has an added dimension: orchestrating actions needed to protect a company's people, facilities, and information from unimaginable disasters.

2. When was the business continuity plan last updated? For example, e-mail used to be something that no one was really dependent upon, whereas today, few businesses can operate without it. If the business continuity plan is more than three years old, e-mail is probably not on the recovery tree. If the CEO knew that was the case, he or she would change it right away.

3. How often is the recovery plan tested? The answer should be semiannually, even sooner if major modifications have been made since the last test. Many CEOs would be concerned if they knew how many parts of their enterprises fail to test a disaster recovery plan in advance or how many in their management ranks underestimate the real time to recovery.

Finally, and of the greatest importance,

4. Have we ever passed the test? Unfortunately, it turns out that most of companies with business continuity plans have not.

If the answer to any of these questions is unsatisfactory, the board's audit committee should be looking at the business continuity plan on a regular basis until they are convinced it has been fixed.

Board members, through delegation to senior corporate officers, must ensure that line executives understand both the market forces and technology trends that are affecting business continuity requirements. These executives must recognize the significance of networked storage to future technology initiatives and need to accurately assess the implications of delivering business continuity throughout their organizations.

CONCLUSION

Today, information must reside in multiple copies in multiple locations on different combinations of hardware and software platforms. It must be managed proactively and automatically from the second it is created until it is deleted or permanently archived.

In the wake of the catastrophic events of September 11, global corporate leadership today has an added dimension: orchestrating the breadth of actions needed to protect a company's people, facilities, and information from once unimaginable disasters. Business continuity is no longer just an information technology responsibility; rather it is a business responsibility as well. In fact, business continuity and shareholder value have never been more tightly linked. ■

NOTES

1 One estimate places the increase in cost to the U.S. economy from attacks to domestic information systems at 400 percent over four years. The White House, "The National Strategy to Secure Cyberspace" (February 2003), 10.

2 Estimates from EMC Corporation, 2003.

3 IDC Corporation as cited by David Purdy, "Productive Protection: Business Continuity That Delivers Strong ROI," *Continuity Insight* (March 2003).

4 Merrill Lynch and McKinsey & Company, "The Storage Report—Customer Perspectives & Industry Revolution, A Joint Industry Study by McKinsey & Company and Merrill Lynch's Technology Research Group" (June 19, 2001), 50, <http://optistortech.com/WEB%20Library/Industry%20News/McKinsey_wp_20010619_TheStorageReport.pdf> (accessed April 10, 2003).

5 Tim Schmidt, Encore Consulting Group Inc., GartnerGroupDataquest research, "The Infrastructure That Supports Infrastructure," a CRM magazine White Paper, 3, <http://www.emc.com/pdf/continuity/emc_crm_wp.pdf> (accessed April 10, 2003).

6 Hot site providers are service providers that offer their customers, on a subscription basis, access to backup data centers and office space, as well as computing and networking capacity for business continuity and disaster recovery.

7 Fail-over is the ability of a system to automatically, and without human intervention, engage a backup component or system in the event the primary system fails, thus ensuring continuity.

8 Eric Chabrow and Martin Garvey, "Playing For Keeps," *InformationWeek* (November 26, 2001), <http://www.informationweek.com/story/IWK20011121S0005> (accessed April 10, 2003).

9 TechTarget Network, searchStorage.com, "Bank avoids data disaster on Sept. 11," March 6, 2002, <http://www.emc.com/continuity/related/searchstorage_0202.pdf> (accessed April 10, 2003).

10 Ibid.

11 Tim Schmidt, Encore Consulting Group Inc., "Beyond Disaster Recovery: Architecting a Business Continuance Solution Capable of Yielding Real Business Value," 2000, 32, <http://www.emc.com/pdf/vertical/bk2k_recovery.pdf> (accessed April 10, 2003).

12 Ibid., 33.

13 Wendy Cholbi, "Contingency Planning: What Every Director Should Know," *Bank Director* (1st Quarter 2002), 43, <http://www.emc.com/pdf/news/bankdirector_q102.pdf> (accessed April 10, 2003).