WHAT TO PROTECT AGAINST? DISASTER AVOIDANCE VERSUS DISASTER RECOVERY

by Gene Kern

Avoidance, Recovery, Continuity

Businesses can be interrupted by events as simple as a network outage, or as devastating as a tornado, fire, or even an act of terrorism. The most appropriate step you can take to reduce the impact of a disaster is to first realize that it could happen to your business.

Let's make sure we're all on the same page, definition-wise. *Disaster Recovery* (DR) describes the strategy an organization employs to deal with potential technology disasters so that the effects will be minimized and the organization will be able to either maintain or quickly resume its mission-critical functions. It follows then that Disaster Recovery Planning (DRP) needs to focus on the data, hardware and software critical for a business to restart operations that have been shut down by a disaster.

Disaster Avoidance, as the name implies, is the process of *preventing* or significantly reducing the probability that a disaster caused by humans, machines, or forces of nature will occur; or if such an event does occur that the effects upon the organization's technology systems are minimized to the greatest extent possible.

Business Continuity (BC) procedures kick in as soon as a disaster is triggered. These procedures are a progression of preordained tasks, manual or autonomic, aimed at enabling an organization to continue serving its customers during and after a disaster. It precedes, and ideally minimizes or precludes, the recovery process.

Business Continuity Planning (BCP), explained below, is an excellent starting point for a business to focus because it yields valuable input that can be used to develop cost-effective *Disaster Avoidance* policies. The BCP process requires the business to identify its mission-critical operations and indispensable processes and data that are essential to keeping the business functioning as a disaster is occurring. Only by knowing the value of the processes and data you are protecting can you have a basis for effectively allocating dollars towards protecting them with Disaster Avoidance methodologies.

After the BCP has prioritized the key business processes, the next step is to identify the specific and significant threats that could disrupt normal operations. And, finally, devise mitigation strategies to ensure effective and efficient organizational response to the challenges these specific threats create during and after a crisis.

While there are certainly overlapping features and objectives of these three strategies, it's important to understand and benefit from the distinctions, because they are certainly not mutually exclusive. Disaster Avoidance policies and procedures will minimize your exposure to certain disasters. Business Continuity Planning will maximize your ability to keep mission-critical processes working as a disaster unfolds or to resume as soon as possible afterwards. And, the main objective of a Disaster Recovery Plan is to bring operations back as quickly and seamlessly as possible after they have been interrupted by an event.

If the BCP process can cost-justify implementing all three, your business will be positioned to face fewer disasters, experience far less disruptions in operations, and will be prepared to recover more quickly when operations are halted.

The Impetus for Disaster Planning

Business preservation is the primary overriding force that supports all efforts to protect your operations from disasters. The internal need, desire and want to survive that are shared by the company's stakeholders, are constantly being challenged by an assortment of external forces and pressures.

To remain competitive in the marketplace, a business simply can't afford to fall easy prey to disaster-related outages and downtime. Customer service suffers, production halts, product deliveries fall behind, and vital communication channels are disrupted. All of which contribute to lost sales, lost customers, and eventually, unless remedied, a failed business.

As more methodologies emerge to assist companies in achieving increasing rates of uptime, competition intensifies further. Businesses that readily adopt and implement these new disciplines and practices are able to increase market share at the expense of the laggards who are not willing or able to allocate resources towards more diligent disaster planning. Some specific examples of these entities and their methodologies include:

- ***Six Sigma*** is a highly disciplined tactic that focuses value-based strategies to increase marketplace performance, increase customer satisfaction, minimize lead time and reduce costs.
- ***The International Organization for Standardization (ISO)*** specifies requirements for state-of-the-art products, services, processes, materials and systems, and for good conformity assessment, managerial and organizational practice.
- ***The American National Standards Institute (ANSI)*** oversees the creation and use of thousands of guidelines that directly impact businesses in nearly every sector.
- ***The Information Technology Infrastructure Library (ITIL)*** is a globally recognized collection of best practices for information technology service management including DRP and BCP.

Within the last decade, the natural desire to survive is being matched in intensity by legislated requirements to survive. Governmental compliance rules are mandating that companies protect stakeholders by maintaining persistent and on-demand access to, and availability of, data, as well as the preservation of communiqués and other electronic records. Some of the more pervasive regulations that have placed on businesses the demand to implement policies and procedures to maximize data integrity include:

- ***Sarbanes-Oxley Act of 2002***, a result of the large corporate financial scandals, represents the biggest modern change to federal securities laws on record keeping.

- ***SEC Rule 17a-4*** requires that member brokers and dealers preserve all original communications that relate to their business for up to three years with easy access for two years.
- ***Gramm-Leach Bliley Act*** includes provisions to protect consumers' personal financial information held by financial institutions.
- ***1996 Health Insurance Portability and Accountability Act (HIPAA)*** establishes regulations for the use and disclosure of any information about an individual's health status, provision of health care, or payment for health care (Privacy Rule).
- ***USA Patriot Act*** requires financial institutions to implement identity verification procedures, antiterrorism regulations, and capabilities to identify customers and flag suspicious transactions.

And, to add insult to injury, some post-911 and post-Katrina laws are even requiring that data survive even when the business doesn't.

Sources, Perpetrators and Categories of Disasters

Be sure to pick your battles. Because, in the disaster abatement world, everything has a price. Certain types of disasters lend themselves to avoidance. With other types, the best you can hope for is a quick recovery.

Take natural disasters, for example. They can't be avoided. No amount of preparation will stop an F4 tornado from running through your community or flood waters from breaching a levy. They're going to happen, so a Disaster Recovery Plan is just smart business. The more exposure to natural disasters your business experiences, the more resources you'll need for DR.

Fortunately, natural disasters, which wreak the most havoc, are also the least common. While frequency statistics for the various sources of disasters differ greatly, depending on their source, there is one recurring conclusion among them all – human error is a major cause of disasters that lead to data loss (32% according to *Strategic Research Corporation*). Collectively, SRC sites hardware and software failures as the leading cause at 58%. Virus attacks are the culprits 7% of the time and, as expected, natural disasters are responsible for only 3% of data loss incidences.

FEMA, which is primarily concerned with the most serious of disasters that effect communities or even greater geographic areas, focus almost all of their energies on three major sources of disaster: Natural causes (meteorological, geological, celestial), human error, and more recently, terrorism.

Ultimately, most studies agree that human behaviors, whether accidental or intentional, will continue to be a leading cause of disasters. When you combine these with mechanical and software failures you are accounting for the vast majority. And, fortunately, many of these can be prevented by implementing *Disaster Avoidance* procedures.

Procedures, Processes and Reporting in a Perfect World

It's the good news/bad news scenario. The good news – fairly capable technology is available for implementing very effective avoidance, recovery and continuity strategies. The bad news – the DR and BC responsibilities are very often managed too low within the organization, with disparate lines of reporting, to yield a cost-effective, optimum implementation of the technology. Normally, DRP is under the auspices of the IT department, while *Business Continuity Planning* can be found within a business unit, operations, or even managed by corporate security.

The result of this scenario will often be a collection of disjointed plans that exhibit superfluous spending and unproductive duplication of efforts. Since there is much overlap in the tasks and resources required to achieve the objectives of DRP, BCP and even Disaster Avoidance, all would benefit greatly from a coordinated, integrated process.

Imagine how streamlined and efficient these plans could be if they were developed by a committee comprised of professionals from

Disaster Recovery Tier Definitions

Criticality Tier	Corporate Impact Description	RTO	RPO	Minimum IT Requirements	Minimum Facilities Requirements	Costs	Data Center Tier
Tier 1	**Mission Critical** Applications defined as being of a critical nature to the success or failure of the corporation	4 hrs	≤ 1 Min	Virtualized Server Environment Geographically Disbursed Clustered Servers Geographically Disbursed Clustered Database Geographically Disbursed Mirrored SAN	Redundant Power System Redundant UPS Redundant Dedicated HVAC Redundant Generator Redundant Fuel Systems Sites Hardened	$$$$$	Tier IV
Tier 2	**Enterprise** Applications or systems defined as impacting the entire corporate environment or a very large % of employees		≤ 1 Min	Virtualized Server Environment Geographically Disbursed Clustered Servers Geographically Disbursed Clustered Database Geographically Disbursed Mirrored SAN	Redundant Power System Redundant UPS Redundant Dedicated HVAC Redundant Generator	$$$$	Tier III
Tier 3	**Departmental** Applications impacting a single department but not defined as critical	24 hrs	≤ 2 hrs	Locally Clustered Servers Locally Clustered Database Locally Mirrored SAN Storage	Redundant Power System Redundant UPS Redundant Dedicated HVAC Redundant Generator	$$$	Tier III
Tier 4	**Local** Applications impacting a single location or small group of users or individuals in differing departments	72 hrs	≤ 36 hrs	Redundant Power Supplies (even numbers) Local Database Local Storage Data and OS Backed Up	Redundant UPS Redundant Predator HVAC Dedicated Power and Cooling Generator	$$	Tier II
Tier 5	**Other** Applications that are not vendor supported, run on out dated OS, are legacy apps that are just reviewed for data, kept to meet regulatory requirements, or are used by a very small segment of the corporate population	≥ 1 week	≤ 1 week	Single Power Supply Single Server Database on local server Local Storage Data Backed Up	Dedicated Power Dedicated Cooling Conditioned Power (UPS)	$	Tier I

multi-disciplines – engineering, finance, operations, IT, and facilities management. And, what if this committee had direct reporting responsibility to a C-level executive? Optimum planning, with top-level buy-in, would certainly maximize the successful results when these strategies are ultimately implemented.

As for the overall process, *BCP* is the most logical starting point, since it includes a *risk assessment* that assigns to each category of disaster, a probability of occurrence over a specific time span. It also defines the impact each type of disaster would have on the business.

Another outcome of the risk assessment is the identification of *Recovery Time Objectives (RTO)*. The RTO specifies how long a particular system can be down before having a major impact on the business' ability to survive. The third benefit of the risk assessment is the determination the Recovery Point Objective (RPO) for each application/system. The RPO identifies how much data can be lost before the business is unable to recover the system in question.

From the RTO, RPO, probabilities of occurrence, and identification of affected systems, an *hourly rate of downtime* can be calculated. At this point, finance and accounting processes are used to cost justify proper levels of spending for disaster avoidance, disaster recovery and business continuity. And finally, assuming the committee has a direct line of report to a C-level executive, approval by a chief decision-maker can more easily be obtained after presenting the resulting recommendations and supporting empirical data.

This is the process that would unfold in a perfect world. An ambitious, but worthwhile goal to aim for.

An Ounce of Avoidance...

Perhaps the only thing more important and cost-justified than a well documented Disaster Recovery Plan is a well devised Disaster Avoidance strategy and a well implemented disaster avoidance architecture.

The most effective disaster avoidance architecture will be impacted by the previously defined requirements and commitments for business continuity, which include budget, resources and management support.

Disaster Avoidance planning assists in understanding the costs and benefits of various architectures through careful consideration of certain key inputs derived from the BCP, including…

- How much redundancy is possible in your application architecture?
- What is your desired Recovery Time Objective (RTO), defined as the amount of downtime that can be tolerated in the event of a disaster?
- What is your desired Recovery Point Objective (RPO), defined as the amount of data loss that can be tolerated in the event of a disaster?

So, what constitutes a well implemented disaster avoidance architecture? Some of the basic elements include:

- Fully-redundant power and environmental systems in all data centers
- Comprehensive disaster recovery plans for each data center
- Annually executed internal and external Disaster Recovery audits
- Perimeter system security consisting of firewalls, virus protection, Spyware prevention and persistent patch management
- Physical alarm and security systems, peripheral security with video surveillance, access security
- UPS and emergency generators

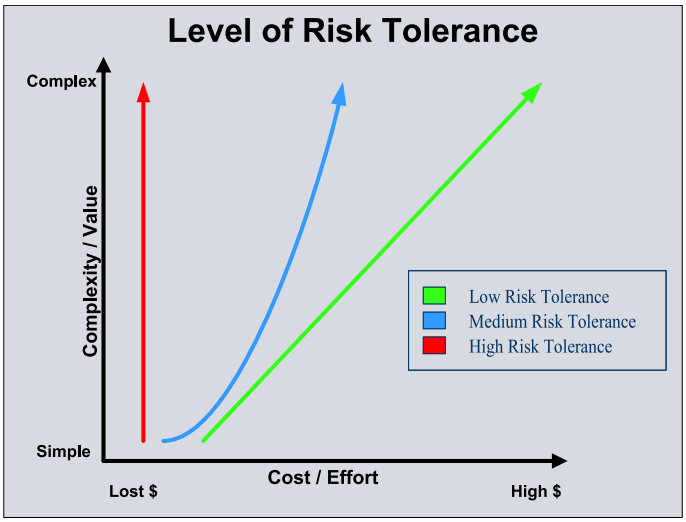
Since we define disaster avoidance as taking all feasible steps to safeguard the physical, informational, and communication assets of the business, where the risk assessment findings determine there is cost-justification, a disaster avoidance architecture can also incorporate a wide range of state-of-the-art technologies, including:

- Enterprise-class, fault-tolerant servers with high 9's availability
- Mainframe technologies, which still provide reliable fail-over capabilities
- Data vaulting, replication, and mirroring
- Fail-over software technologies
- Virtualization, which allows for rapid provisioning of application instances
- SAN storage replicated between sites
- Highly availability systems designed in clusters

Is an ounce of avoidance worth a pound of recovery? Consider that each dollar spent helping the business achieve disaster avoidance, is just that, a dollar spent. But, a dollar spent on disaster recovery, doesn't end there. Far more dollars will be consumed during the outage than will be spent preventing it.

Summary

With modern day global unrest, global warming, and global competition, mitigating the impact of pending disasters isn't a discretionary endeavor; it's a matter of survival. And, the optimum approach is to adopt coordinated strategies for disaster avoidance, disaster recovery and business continuity, since each plays a unique role in the preservation of the business.



Gene Kern is Executive Vice President of WAKE Technology Services, Inc. He can reached at gkern@waketsi.com

Note: The information, links and related content are compiled as a reference and are in no way endorsement by the chapter, its officers or the national organization. Please use the information as you see fit and feel free to contact the author for additional clarification. We strongly suggest that information you reference be cross validated with alternative sources.