Beyond the Year 2000

Developing a Business Survival Plan

The Year 2000 has, if nothing else, made some people aware that there are risks to their businesses.

Unfortunately for many, they view the "Y2K bug" as the only risk.

It is not. Tune into any radio or television station, pick up any newspaper or magazine and you are confronted with a variety of disasters -- in Florida, weather-related events get the most attention.

Most businesses have some type business plan.

Most business plans, sadly, fail to include a **business continuity plan**.

Business continuity plans, also known as business contingency or disaster recovery plans, are **survival plans** for business.

Any business.

Every business.

Commercial and industrial operations, non-profits and charities, and governments at all levels.

There is some argument about that constitutes a "disaster." This scrivener considers a disaster *anything that causes injury or death to personnel or causes a business to fold.*

The purpose of a business continuity plan is to make certain the business survives a worst case disaster condition. What is "worst case?" As Norm Harris, one of the planning industry's founders, put it, the worst case is "going to work and finding there is nothing there."

Planning for the worst prepares for anything less.

Basic steps

Professional planners know there are several "basic" steps to include in every business continuity plan. The steps include

- defining business functions
- identifying risks to those functions
- ranking the risks by impact and probability
- identifying, and implementing, measures to avoid or mitigate the risks
- determining recovery procedures in the event a disaster condition occurs

Unlike many things, continuity planning requires -- demands -- that top management enthusiastically support the plan; lip service or luke-warm support will result in a plan that is guaranteed to fail.

Define business functions

Many managers, when asked what they need to protect, respond: “the computers and the computer network.”

So far so good.

But consider a manufacturing operation. If a flood destroys the production line, there are no new products made. Once any stockpile is depleted, there is no income. Production line personnel are laid off. Then support personnel - A/R and A/P, HR, development personnel, eventually management - are downsized.

There is a further ripple effect. The laid off personnel will soon be unable to pay their bills to local merchants and financial institutions, forcing those vendors to lay off personnel for lack of revenue.

While there are priorities in the *recovery* process, each individual, albeit not independent, business function must be identified. What is the function; what is accomplished by the function; how is the function accomplished to a fine level of granularity.

Identify risks

Every business function has associated risks.

Professional planners know the risks are not always obvious.

Everyone understands the risks posed by hurricanes, but not everyone considers what can happen if a vendor fails to deliver on time or a trucking firm’s employees strike. (Does anyone remember the United Parcel Service strike? FedX and U.S. Postal Service people do -- they suffered under an added workload and gained some additional, long-term business at UPS’ expense.)

Risks come from every corner and the list is lengthy.

Flooding, it turns out, is the number one risk throughout the United States according to the Federal Emergency Management Agency (FEMA). (Debris clean up is the number one expense.) Given that, one wonders why a company would first build on a flood plain and then put its income-generating business function on the first floor of a multi-floor structure. But it happened.

Analyze and rate risks

There are risks and there are risks.

Some are so likely to occur that it is wise avoid or mitigate the risk.

Some, while not likely to occur, could cause so much damage that something must be done to avoid or mitigate the impact.

Some are unlikely to occur and even if they do occur, would cause only minimal damage; these risks fall into the "absorb" category, the "we'll deal with if it happens" category.

Flooding is a "likely to occur" risk. Since flooding often has a major impact on a business - who is foolish enough to use electrical machinery when they are standing in water? what computer system is designed for "underwater operation?" - the planner looks for ways to avoid the disaster condition (build about the surge level, put critical equipment on upper floors of a multi-story structure).

Tornadoes are less likely to occur than flooding, but the devastation wrought by a twister is immense. Granted, Florida is hardly a tornado alley compared to Oklahoma, but they typically tag along with hurricanes and hurricanes **are** a fact of life in the Sunshine State.

Since there is little to be done to prevent tornado damage to a structure, the planner must find ways to mitigate damage to the business. Often, this is accomplished by arranging for a back-up operation in another location and making certain the building has appropriate insurance coverage.

Some risks are too unlikely to occur or, if they do occur, will cause only minimal inconvenience; these risks are "absorbed." Typical of such a risk is a desktop computer. Given the speed technology is advancing and equipment prices falling, most businesses would allow desktop computer **hardware** to fail. This does **not** apply to the data on the desktop machine which must be protected.

Identify, and implement measures to avoid or mitigate the risks

Once the risks are identified and the probability of occurrence determined, means to avoid or mitigate the risks can be examined.

Most risks have many options; each option has its own pluses and minuses. In general, the greater the protection, the greater the cost.

Management must decide each business function's value to the business to determine what risk management (avoid, mitigate, absorb) option to take and, in the case of avoidance and mitigation, how much it is willing to spend to implement the protective measures.

Determine recovery procedures

Once avoidance and mitigation measures are implemented, a "sub-plan" is written to define the recovery procedures.

The plan starts with declaring a disaster condition and ends with a declaration that the business functions have been restored and "business as usual" has resumed.

Built around a **disaster recovery team**, this plan assigns specific tasks to specific personnel and covers the complete range of business functions. It may include use of vendors to provide a variety of services ranging from clean-up to out-of-area housing.

Tailor the plan

While there **are** *basic* business continuity plans available on the Internet, each business, even each business location, should have its own, tailored, plan.

Each business and location has a unique "personality," even when everything is created to a "cookie cutter" general scheme. There are too many influences - weather, municipal codes, local culture, and more - beyond the control of "cookie cutter" plan.

Having a certified planning professional create a business continuity plan is not an absolute requirement anymore than having an insurance professional provide guidance on insurance or a physician offer an opinion on health matters. It is not a requirement, but it does make good sense.

After the plan

Before putting -*30*- to this, there are three remaining things that must be done to create a viable plan to help your business survive.

First, **test the plan**. I have never seen a perfect plan the first time it was tested. There is too much chance of an "Oh, I forgot to mention …" and "We changed this after talking to the planner, so …" *Things* happen, that is inevitable.

Second, **publish the plan**. Make certain everyone knows there is a plan and their role, if any, in the plan. "Everyone" includes your vendors and clients and, if yours is a public company, the stockholders.

Third, **maintain the plan**. People change. Policies, processes, and procedures change. Equipment is replaced. The plan must be modified regularly to reflect these changes, and then it must be tested.

Y2K - tip of the iceberg

The Y2K problem is just the tip of the risk iceberg. Since it made you aware of that risk, seize the moment and take the steps necessary to protect the entire business from all the risks lurking outside the door.

Protect your company and help protect your community.

The bottom line for disaster continuity planning is survival.

Survival of personnel.

Survival of the business.

No matter **what** the business.

John Glenn, CRP, is a certified business continuity planner and a consultant with the Tampa office of DMR Consulting Group Inc. Glenn creates disaster recovery and business continuity plans for government and Fortune 200 companies throughout the Southern U.S. In addition to his professional certification, he also holds several achievement certificates from the Federal Emergency Management Agency (FEMA).