CPA
Practice Advisor

ADVISORY

An Executive Primer on Business Continuity Planning and Related IT Considerations

Robert P. Green • Sep. 01, 2009

The following terms are undoubtedly familiar to you: Disaster Recovery, Disaster Preparedness, Business Continuity Plan, Operations Resumption Plan.

But how do they relate to you or your clients? Moreover, how does information technology fit into these concepts?
In the big picture, the above terms all emphasize the survival strategies in a business' Risk Management process. In a more perfect world, every company would prioritize the strategic and tactical processes required to resume, sustain and manage their operations through an unplanned disaster or a damaging business interruption.

Many constituents have a legitimate interest in this Risk Management process, from employees and management to owners and investors, and outside parties such as auditors and bankers. As such, why don't most businesses, particularly those that are not SEC registrants, prioritize this matter?

First, it is a great deal of work to become proactive and to determine the activities required before any disaster, as well as to be able to plan the processes to resume after a disaster. Business Continuity Planning (or a Business Continuity Plan), which is also referred to as "BCP" is indeed challenging

... and is far more involved than just drafting an insincerely prepared plan and filing it in a drawer. Second, most businesses don't have the internal management experience to address this process. And third, among others, many business owners and managers believe that their business is already prepared for disasters based on naïve assumptions such as "we have good backup tapes" or "we know everyone's cell phone numbers." And then you have the other thought process (which is often unspoken) that summarizes many business' approach to this risk: "It won't happen to us."

BCP involves company-wide participation, coordination with internal and outside constituents, ongoing updates, management and testing. Among the most critical components of the BCP process, however, and among the more straightforward to address is the ability to have information and computer systems survive and support the business as a result of some disaster.

Information technology is a key driver in BCP. Without considering the IT factors, a disaster can dramatically impact a business' continuity in the form of lost data, lost practices and automated processes, lost revenues and lost operations. Read on for an example of what can happen.

Imagine This Horror

Your client, ACME, runs a business with five offices spread around the country. A snapshot of its IT environment is important to be aware of in our example. From its headquarters, ACME manages its operations, accounting, IT network and all software services for its five offices. ACME also hosts its own website, eCommerce and all data servers at its headquarters. Forty percent of ACME's business originates from customer transactions using ACME's website. Finally, as a good business practice, ACME does not allow its system users to backup or store documents and other sensitive data on their own computers. Rather, their information is centralized in ACME's servers at headquarters to ensure (we'll see) comprehensive backup.

ACME's headquarters was hit by a relatively harsh storm. The lower floor, which houses the server room, flooded to a good degree due to a leak caused by ineffective weather preparations. The flood caused irreparable systems and hardware failures. Work came to a halt ... in all locations. The client website was completely "down," precluding many customers from conducting business with ACME. The most recent backup tapes were over two weeks old and

were actually stored in the server room. Sadly, they were ineffective because they were soaked and damaged by surrounding debris. A search continued unsuccessfully
for other reasonably current backup tapes.

Dilemma: No current data. No productivity. Limited customer orders and interaction. No likelihood of restoring any current or perhaps ANY information with which to do business.

Exaggerated? Not sure how realistic this is? Perhaps, then, substitute for "flood" other real disasters outside of natural occurrence — ACME's confidential and private customer data and trade secrets could have been compromised by a disgruntled employee or other insider or the servers could have literally been stolen by a competitor or enterprising employee. Other disasters in the Mother Nature category that can yield the same result include power surges, earthquakes and isolated or wide-spread fires. All of these occur somewhere every day.

Avoid The Horror

Define and tackle your objectives for Preparedness and Resumption

Engage in BCP; it allows a business's operations to resume (as planned) after a disaster. A BCP for any business should address IT considerations, as well as others: human resources, media or press relations, emergency response agencies, operational and physical logistics, and more. Even if ACME had only accomplished some BCP, surely some of the above risks would not have had such business-halting results.

If businesses resist engaging in BCP because they choose to avoid its common sense and prudence, then consider this: BCP efforts are addressed (directly or indirectly) in regulatory compliance doctrines in place today for companies of all sizes, from Sarbanes-Oxley to HIPAA and other Privacy Protection acts, both Federal and local.

BCP efforts require a significant investment of corporate labor, outside advisors and financial resources, and include efforts of procedure design, implementation and testing. Objectives and tactics of BCP follow, with an emphasis on IT considerations.

Creating, Maintaining And Testing The BCP

First, the plan must be created. We recommend that a BCP/crisis management team be formed and empowered to create, manage and update the BCP. This team should represent all key departments, and focus on the following objectives:

- the continuity and survival of the business,
- the protection of corporate tangible and intangible assets,
- human resources and 'public' awareness of the event,
- the creation and documentation of specific preventative measures/activities, and
- the ability for the BCP to be effective, as a whole, on an ongoing basis.

At its core, a BCP addresses the myriad of business risks that a company would face in the event of foreseeable disasters, including the nature of disasters as well as the most important risks of loss. A business must determine the following at the onset:

1. What kind of disasters are most likely to impact the business?

a. Natural disasters – the usual suspects might include fire, flood, earthquake, and the like.

b. Human-oriented disasters – including theft of digital intellectual property and trade secrets, or compromising of web commerce activities, stolen servers, etc. Others include carelessness resulting in a lost unprotected laptop or flash drive containing sensitive information, as well as inappropriate or ineffective network and security design and management.

2. What attributes of a disaster are most impactful to the sustenance of the business' operations?

a. Loss of the business' website and eCommerce capabilities.

b. Loss of Internet access for extended periods of time.

c. Loss of power to keep IT and other operations equipment running.

d. Loss of email access or file/folder access.

e. Loss of employees to conduct business due to geographical or pandemic disasters.

f. Loss of strategic data (customer lists, accounting data, sales information, other intellectual property, etc.).

After addressing the above, the BCP starts to take shape right away. The BCP team creates action plans and documentation of procedures that address and mitigate
each of the risks related to the disasters most likely to be impactful … and then tests these plans and procedures "real time" to the extent possible. This may mean shutting down the company's power or Internet connectivity during business hours. Many companies do NOT test their planned procedures in any way, nor update them as information and the business changes. Thus, the BCP may be entirely useless at the actual time of need.

How ACME Could Have Prepared Better

A BCP at ACME should have included better IT preparations. Some examples of procedures might include the following:

1. Regular and secure offsite rotation and storage of data backup tape(s), accompanied by procedures on how to retrieve them and restore data and systems functionality from them.
2. A duplicate eCommerce website environment "at the ready" that activates when the primary site fails for any reason. This could be located at any number of other locations, including a sister office, or a third-party Internet host.
3. Offsite or remote server redundancy. Examples include:
    - A "hot site" – an off-site duplicative server and system environment that allows for resumption of systems operations, with the ability to be connected "live" upon instruction. This approach is simplified and often most effectively managed using a newer technology known as Virtualization of the server environments, which allows for more simple and affordable redundancy.
    - The adoption of an externally hosted 'cloud computing' server and data environments. In this "cloud" concept, a company's servers, software and data are hosted by third parties and served to the users via an Internet browser on any computer. Hence, resumption would occur simply by finding an Internet browser anywhere.

4. Redundant Internet and telephone services. Alternative Internet connection services can activate automatically upon a disruption of the main connection, thereby keeping communications alive without interruption. Secondary phone systems or Internet-based phone systems can be made available for those incidents when communications failures occur.
5. Effective server room construction and configuration. Considerations include adequate levels of air conditioning, drainage systems, weather proofing, ceiling leak testing, etc.

Summary

BCPs are critical in today's business climate, and the businesses that invest time and effort in their creation, maintenance and testing are well rewarded in the event of disasters and disruptions of any kind. Specific information technology practices for avoidance of data loss from disasters are increasingly necessary to make BCPs successful and effective. And they are very affordable and achievable when addressed prudently and in advance. This enables BCP constituents
to more likely enjoy the peace of mind that they deserve.

Robert (Bob) Green, CPA.CITP/Partner and Rick Mark/Senior Manager are Information Management professionals in the Enterprise Risk Management Services group at SingerLewak, LLP, one of the western U.S.'s largest CPA and consulting firms with six offices in California. This group provides CIO and CTO advisory services, as well as governance, risk and compliance advisory/audit services to privately held and SEC registrant enterprises. Bob presently serves on the AICPA's Certified Information Technology Professional credential committee. They can be reached at BGreen@SingerLewak.com and RMark@SingerLewak.com.

Advisory • Technology