Global Information Assurance Certification Paper

Business Continuity: Where Do You Begin?

GIAC Security Essentials Certification Practical
Version 1.4b (Option #1)
By Sean Crook
Date 5/31/03

Abstract

How many times have you heard "That'll never happen here" or "We've been doing it this way for years and nothing has ever happened to us?" For many, hearing these statements makes us cringe. The events of September 11th changed many things, but Business Continuity was not one of them. Sure, it was a buzzword for about a year, but then things started to quiet down. Now companies that have never bothered to develop a Business Continuity Plan (BCP) have once again put it on the back burner.

Why is this? It could be time, money, or both. Whatever the case, there really is no excuse for not having a BCP. A BCP should be one of the most critical pieces of the organization but sadly in many cases, it's not. The BCP is a long process that never ends. My goal is to discuss how to convince senior management of the need for a BCP. I will also focus on the first few steps to take when developing the BCP - as these first few steps are crucial.

Introduction

The tragedy that occurred in the United States on September 11th will never be erased from our minds, and it will be embedded in the minds of generations to come. As soon as news spread of September 11th, many were confused and had many questions. The major question being, "How *could* someone do this to the United States?" Talk of war immediately started as President Bush said while talking to rescue workers at 'Ground Zero' with a megaphone, "I can hear you, the rest of the world can hear you, and the people who knocked these buildings down will hear **all** of us soon" ("CK"). It was a moment in this country's history where we united and became patriotic - which hadn't been apparent in many years.

Over the next few weeks, we heard stories of businesses that were destroyed in less than one hour with no backup plan in place. The company Cantor Fitzgerald, which was in the WTC, lost over 700 of their 1,000 employees (SANS Security Essentials 1.2).

Business Continuity gained considerable popularity after September 11th, but now the importance has escaped many organizations. It's not talked about as frequently since September 11th. Many companies are wiping the sweat off their brow and continuing with business as usual. Why is that? It usually comes down

to two areas which are: lack of time and/or money. Companies usually don't have adequate resources in these rough economic times to assemble a BCP, when in reality, companies can't afford to **not** have a BCP.

The mentality is to be reactive instead of proactive. When dealing with confidential data or systems that need to be up 24/7, it's a risk you can't afford to take. Some businesses would prefer delay compensation for a tragedy after it happens as opposed to protecting themselves in case something does happen. What many have unfortunately discovered, it's too little too late.

Pre-Planning

The best way to start is to develop a pre-plan that will roughly map out all the activities that will be involved at a high-level; from the planning until the testing phase and also the upkeep of the BCP.

The consensus among experienced business continuity planners divides the process into seven phases:

1. Project Initiation (New or Enhanced Function(s))
2. Risk Analysis (Determine Vulnerabilities)
3. Business Impact Analysis (Determine Priorities for Recovery)
4. Build the Plan (Develop/Choose Strategies, Write the Plan)
5. Test and Validate the Plan (Exercises/After Action Reviews)
6. Modify and Update the Plan (Plan Improvements, Updates)
7. Approve and Implement the Plan (Get Management Signoff and Train) (Arata et al. 11)

This shouldn't be seen as a checklist of what to do, but more of a guide. Once phase 7 is completed, that doesn't mean it will be done and the BCP can be locked away. This is an on-going process that needs to be reviewed periodically and if anything new is added, the whole process should start again to ensure the plan will work.

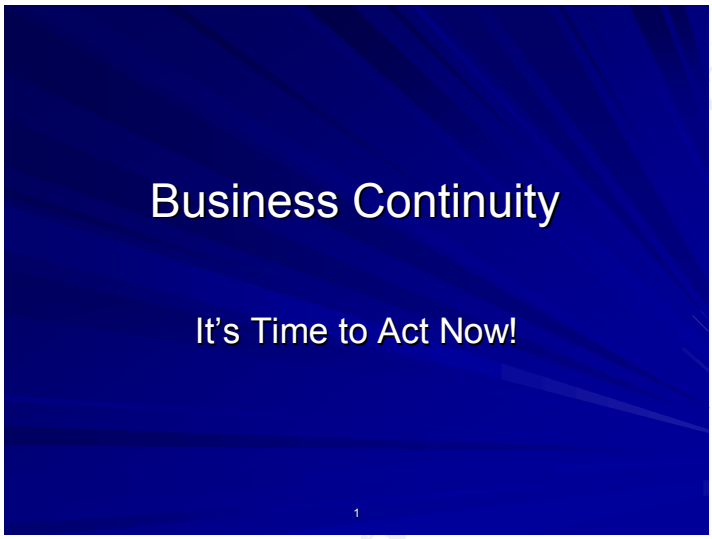
Planning is the most important part of any undertaking. Without a good plan, you're just wasting time. By ensuring that all those who need to be involved are involved, the planning process will run smoothly and should carry over to the other phases of the BCP.

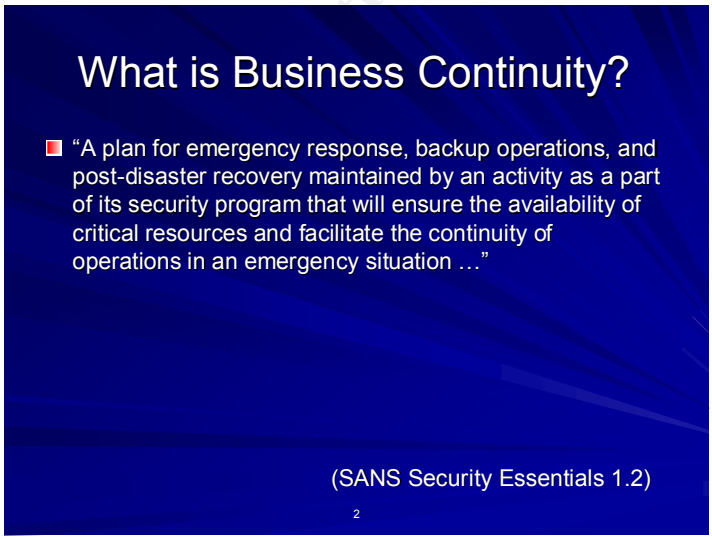
Where to Begin!?!?

You've thought all along that the organization you work for needs a BCP. You're now in a position to bring this to the attention of senior management and hopefully make this a company-wide initiative. The first thing needed is to convince senior management that a BCP initiative is a benefit to the company and its customers. How can this be done? The easiest way to do this is to call

an off-site meeting and present your case. If you have the meeting off-site, it will put focus on the matter at hand and increase the chances of getting your BCP approved. Try to reserve a room with no windows and little distraction so that you have everyone's full and undivided attention. Bringing in snacks and beverages will also earn you some points in getting your plan approved.

The presentation should be high-level and not flooded with technical detail. It should also be short and to the point. Try to keep the presentation time between 30 and 45 minutes. Any longer than this and nerves will start to shorten and attention spans will drift. The best way to make your presentation concise and to-the-point is with statistics and graphs. These are helpful not only to condense material in your presentation, but to also drive the point home as to why your company needs a BCP. Here is an example of some slides you could integrate into Microsoft Power Point (not too detailed but to the point):





Who will be involved?

- Contact the following areas for staffing:
  - "Hot Site" Team
  - Legal
  - Human Resources
  - IT Security
  - Building/Physical Security
  - Public Relations
  - Vendor Off-Site Team
  - Investigation Team
  - Storage Management

(Arata et al. 14)

3

Why do we need it?

- According to a Gartner study, two out of five companies that experience a disaster will go out of business in five years (Arata et al. 8).
- A 3M study done in 1995 showed that in the course of "normal business operations", 30% of computer users spend one week per year reconstructing lost data (Arata et al. 8).
- According to the U.S. Bureau of Labor, of those companies experiencing major service outages, only 6 percent survive long term, 43 percent never resume business, and 51 percent shut down within two years (Wilson).

4

Benefits

- Assists in identifying critical and sensitive systems
- Provides for pre-planned recovery by minimizing decision making time
- Protects your organization's assets and employees
- Minimizes potential legal liability
- Reduces insurance premiums
- Satisfies regulatory requirements, if and where applicable

(Arata et al., 6)

5

As stated earlier, it seems the events of September 11th have been looked at as a one-time event. It has been almost two years since the attack and many companies still don't have a BCP. This unfortunate reminder will help demonstrate the need for a BCP.

The fact you don't have a BCP is probably because it's never been presented as a necessity to senior management and this presentation will help bring this to their attention and take notice. With any luck this slide show will spark a good Q&A session and after some additional discussions, senior management will agree that a BCP needs to be your company's top priority. Odds are, since you were the one who came up with the idea, you'll be the one to organize the effort. So what do you do next?

Business Impact Analysis (BIA)

In order to develop a good business plan, you'll need to know which areas of the organization need to be involved. Using a Business Impact Analysis (BIA) can do this. Businesses need to decide what is most important or vital for their operation and determine how much they want to spend to protect that asset. The best way to do this is at a high level with senior management since they determine the direction of the organization. Then you can proceed with each business area and let them determine what is critical since they'll know better than anyone (even senior management). Once it's determined which areas are critical and need to be part of the BCP, you'll be able to contact those areas to develop the core team.

Here are additional detailed examples of questions that could be deemed important to maintaining an organization's operational stability:

1. Does your network include redundant intelligent network routers that can switch processing workloads to another system or node when one fails it becomes overloaded? *It is sometimes overlooked but insufficient system capacity can lead to downtime. Having redundant routers and switches that can overflow onto each other, will accommodate spikes in traffic as well as redundancy in case of failure.*

2. Are your web servers load balanced? *The increase of Denial-of-Service Attacks lately should prompt any large organization to load balance their web servers. By load balancing web servers, intelligent software can manage an increase in web requests by handing them to idle or less busy servers.*

3. Have you designated your business process for growth? *Scalability of the business process is sometimes overlooked and can lead to serious availability problems. Databases will grow in size and quantity, more employees will be hired, web hits will increase. As this happens, bottlenecks develop causing resources to become unavailable.*

4. Do your ASP(s), ISP(s), and other outsourced partners incorporate an equal or greater level of redundancy as your own? *Today there are many Application Service Providers (ASP) and Internet Service Providers (ISP). It is important to ask ASPs and ISPs what level of redundancy can be expected from their site. Are they in a high risk area with no power protection? Questions like this should be asked and a site tour should be taken.*

5. Do you have multiple bandwidth carriers in your datacenter? Make sure they don't use the same upstream provider. *At least two bandwidth providers should be used in a data center. It is crucial to know who their*

upstream providers are. If they both use the same wholesale provider it presents the datacenter with a very dangerous single point of failure. If a common upstream provider goes down, your entire datacenter will be down.

6. Do you carriers come in through separate points of entry to the building? *At least two carriers should be used in a critical business process. When deciding on the placement of the physical cable(s) or satellite dish(es), ensure that both are as far apart as possible. It's not uncommon for a backhoe to cut two redundant network feeds because they are located next to each other.*

7. Are you using clustered servers or clustered SMP-type servers (Symmetric Multiprocessing)? *If a server fails in a clustered server environment, no downtime is experienced because the other servers pick up any additional processing. The drawback to clustered servers is that they lack the processing power of a multiple processor server. Today SMP servers have the ability to be clustered thereby providing the best of both worlds.*

8. Has a component failure impact analysis been performed on your network components to determine which should be highly available? *Before buying anything, a careful analysis must be performed to determine what components of the datacenter require the highest availability. This will ensure that all critical systems are properly protected.*

9. Are there any single points of failure throughout the network that are part of a critical revenue stream? *Any single points of failure must be identified. If the single point of failure is part of a critical system it must then be made redundant.*

10. Do you use hot standby systems? *Cold and hot standby ensures that a dormant system is always available for service, however hot standby will immediately process information at the moment a component fails. With cold standby, you experience a delay in service.*

11. Does your primary network location employ hot recovery capabilities located at an offsite facility, which could fail-over instantly? *Hot recovery in a datacenter will allow a quick transfer of system operation if the primary system should fail. The redundant system may be located in the same datacenter or at a remote location. Hot recovery systems located at a remote site will have a higher availability then those located in the same datacenter.*

12. Are you using RAID arrays to eliminate disk drives as a single point of failure? *There are five different RAID levels which may be used*

depending on your budget. There are advantages and disadvantages to each level. However, whatever method is used, it is highly recommended that it be mirrored. Never put all disks from one volume in one cabinet or rack. Divide them up among different cabinets and racks. Always have redundant power supplies, controllers, and data paths

13. Are your databases partitioned and full redundant to protect data integrity during an outage? *In large corporations there are many databases for many different parts of the company. It is very important to partition databases, by department for example, so that if one database server fails the entire organization won't be affected.*

14. Do you incorporate off-site computer data storage in your network? *Disk mirroring is not a solution for data backup. If a file is corrupted or deleted, disk mirroring will not help. It is crucial for any business to backup its data and store it in a remote data vault. Ideally a data vault should be located in some other city or state.*

15. Have you designated a location for an alternate relocation site for your operations in the event of a disruption? *If a datacenter is faced with a catastrophic disruption, it must continue to operate from a remote location. By having a planned relocation site, downtime will be kept to a minimum.*

16. Do you incorporate remote journaling? *File system corruption usually occurs when a system abruptly turns off while the system memory is writing to the disk. Without remote journaling, the entire file system would be checked which can sometimes take hours depending on the size of the hard drive. Remote journaling will decrease the amount of time a system takes to perform a file system check by more than 99%.*

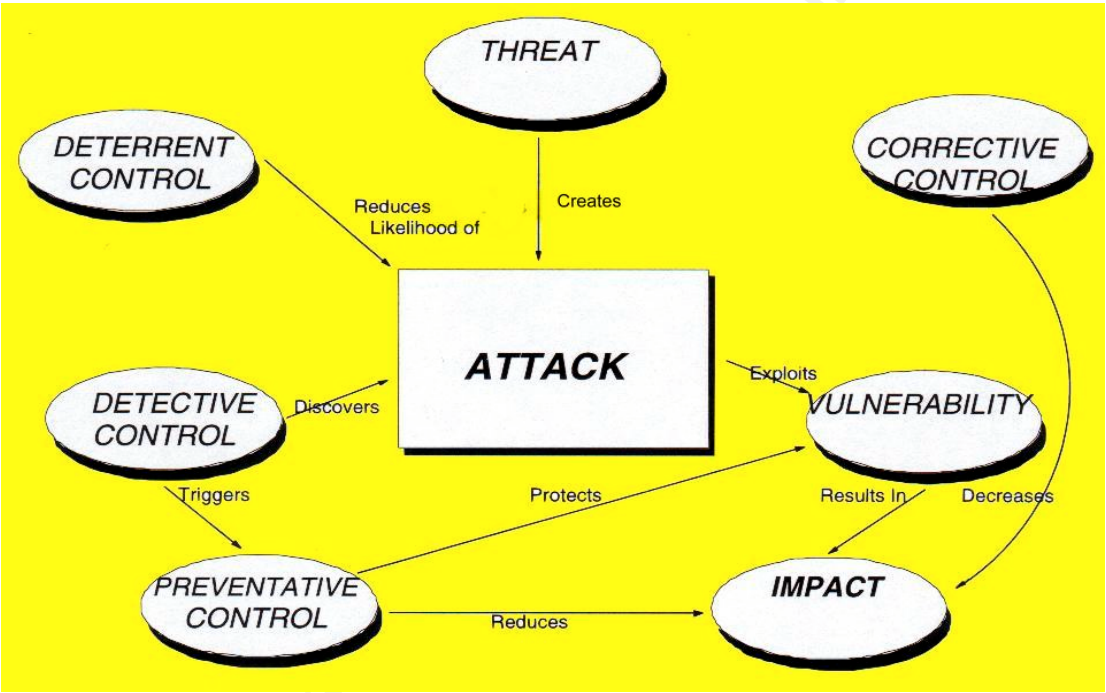
(list taken from http://www.availability.com/elements/information_technology/index.cfm?fuseaction=checklist)

This is only a small list of questions and answers that the organization should ponder. Odds are these questions will lead to other questions as well. When meeting with each area, it's a good idea to have someone there to take meeting minutes as well. After this meeting you'll be able to sort through all of the questions to determine which areas would be impacted the most and need to be involved. Documentation of these meetings is very important. The more you document along the way, the less work you'll need to do later.

Risk Assessment

Once these areas have been identified, proceed with a Risk Assessment (RA). A Risk Assessment takes the risks that have been identified and determines the likelihood that these events will occur. For example, if you're running Windows NT, one server going down may not seem too risky, but if it's the Primary Domain Controller (PDC) of your organization and you're not running a redundant PDC, the risk would be very high. Many places measure risks quantitatively or qualitatively.

Qualitative Risk Analysis is used by determining threats, vulnerabilities, and controls as seen in the graph below:



(graph taken from http://www.security-risk-analysis.com/introduction.htm)

Quantitative Risk Analysis takes into account the probability of an event occurring and the risk associated with that event. The problem with this is who can really predict the probability of a tornado hitting a certain area? Statistics can be collected on events such as how many tornadoes have hit in the last 20 years in a certain area, how often that happens per year, and other statistics. When using Quantitative Risk Analysis, it should be noted that the data is used based on statistics and isn't necessarily the most accurate.

The Approach

Now that senior management has given approval to develop a BCP and you've determined where there's the most risk, there are a few options to choose from:

- Develop and maintain the BCP internally - This is a good method because there are folks involved who already know the business and know what's involved to make it work. It will be easier to identify your critical areas and most importantly, you're keeping the organization's information within the company.

- Develop and maintain the BCP, but hire some third party vendors for certain tasks – This can be a good approach as well. Develop and maintain the BCP, but also hire a 3rd party vendor to perform tasks such as backups or provide supplemental staffing if needed, or give direction on the BCP itself. You do run the risk of an outside company knowing significant information about your company and you may not want to accept that risk.

- Outsource your BCP – There are companies who can provide support, but usually for a high price. Some companies feel they don't have the resources or the time to develop and maintain a BCP, so they outsource it. However, you also open yourself up to a new vulnerability. If for some reason you need to sever ties with this company, they may be bitter and know everything about your organization and can cause significant damage.

For more information on what types of services can be outsourced, here's a list of companies that provide a variety of these services:

- **Commissum** (Security Consultancy) – Commissum helps define requirements based on business critical analysis, managing the business continuity process. (Price: Contact vendor) http://www.commissum.com/operationsandmanagement2e3.html

- **Connected Corp.** (Connected TLM 6.2) – Offered as a host based service or as licensed product software. Connected TLM delivers real-time PC backup, recovery and management for desktop, remote and laptop PCs. Connected TLM's functional modules include Backup and Retrieve, Heal, Asset Recovery, PC Migration and Remote Assist. (Price: $100/seat) http://www.connected.com/

- **Rothstein Associates Inc.** (BCM FRAMEWORK: Comprehensive, Business Continuity Tool) – BCM FRAMEWORK is comprised of a number of easily tailored modules on business recovery action plans for

key corporate actions with organization schematics and role descriptions, with some vital actions included. (Price: $595) www.rothstein.com

- **RSM McGladrey Inc.** (Business Continuity Planning Software (BCPS)) – A Windows-based, user-friendly development tool for a comprehensive business continuity plan. The tool is adaptable for governmental entities to use for development of continuity of operations plans. (Price: $4,000 - $6,000) http://www.rsmmcgladrey.com/index.jsp

- **Solutionary Inc.** (Incident Response Program) – Solutionary's Incident Response Program creates a detailed framework for responding to any event resulting in the loss of access to information, whether through malicious means, hardware failure or human error. (Price: Contact vendor) http://www.solutionary.com/

(list taken from "2003 Buyers' Guide" Information Security Magazine)

As the person in charge of the BCP, you'll need to decide which risks you're willing to take and the consequences of those actions. Keeping it internal is the safest way, but even that isn't a guarantee. Someone internally can become disgruntled and if they're involved in the BCP, they can do as much damage as a 3rd party vendor. On the other hand, completely outsourcing the BCP would mean another company would do most of the leg work but would also know almost everything about your organization. This is a choice you'll have to make and it won't be an easy one. This decision is crucial for the BCP because it paves the way for all the steps to come.

The key point to remember is no matter which approach you take, you'll be the one who is ultimately responsible. You should think it through clearly and take into account all the pros and cons and make the best choice for the organization.

Identification of Core Areas

In any situation, there are areas that will need to be involved 99% of the time. These areas will be considered the 'core' team. The core areas should be limited to those that need to be involved in case the BCP needs to be used. There's no need for everyone in the company to know every detail about the BCP. The areas you choose will be based on your risk analysis, but some areas most likely to be involved no matter what include:

- *Senior Management* – Should be informed throughout the process of the development of the BCP. Senior Management will also need to be contacted should a disaster occur.

- *IT Security* – Ensure that data and systems are secured. This should be done even without a BCP in place however in the event of a disaster; they'll need to take extra precautions.

- *Building Security* – Need to know who should/should not be in the building in the event of a disaster. They will also need to know of any evacuation procedures put into place.

- *Investigation Team* – The Investigation Team will need to be called to determine what caused the disaster and to gather evidence if possible.

- *Storage Management* – You should have off-site backups whether it's part of your organization or a 3rd party. They'll need to know when to start to recover data that may be lost and how far back to start the recovery.

The areas above provide a good starting point, but it will depend on the size of the organization as to which areas are involved. For example, if you're a small organization, you may not provide off-site coverage. If you're a large organization, odds are you'll have many other areas involved. The larger the company, the more difficult the BCP becomes simply because tasks are broken down into their most minute details. If there are 10 people involved, odds are each person knows the others role in the organization. In a large organization the probability of everyone knowing each other's job is unlikely.

Put Together Your BCP Core Team

Now that you've identified the areas that need to be involved with the BCP, you'll need to make a presentation to each area's management. You can do this individually or as a group depending on the size of the company. They may not know what a BCP is or that the organization is even developing it, so you can use a presentation similar to the one given to the senior management.

After you've given the presentation, task the management of each area to determine whom from their area will be on the BCP Core Team. It should be emphasized in your presentation that you'll only need as many as it takes to do the work and select only those they feel would be willing to do the work. As stated earlier, the more knowledge about the plan the greater the risk to the organization.

Once the management of each area has a better understanding of the BCP, they'll need to select the individuals who will be on the BCP core team. These folks will then be tasked with developing solutions for their particular area as it pertains to the BCP.

After the initial selection of the area groups and core team, it would be good to have a preliminary meeting to communicate the basic approach which will be

taken by each group. Some of these areas may over lap each other and to avoid complications, this should be worked out ahead of time.

Your options for BCP training are to hire a high-level professional or contact your learning and development area to develop some training materials.

Common Mistakes

A list of common mistakes should be provided as well. Listed below are some key points:

- *Blindly relying in BCP* – Many organizations believe that just having the BCP is enough. The BCP is only marginally useful without adequate updating, testing, and training.

- *Limiting scope* – An incomplete BCP plan will not address all of the corporate needs for recovery. The BCP plan needs to cover business processes, systems recovery, back office functions, and the replacement of key personnel, if needed.

- *Lack of plan updates* – The BCP should be updated periodically, especially when there are significant system or business process changes.

- *Lack of communications* – There is a need for clear and precise communication with employees, contract employees, vendors, business partners, and clients.

- *Lack of security controls* – During the recovery process, security controls can be disregarded, resulting in a greater risk of exposure.

- *Lack of Public Relations planning* – Companies often fail to consider customer, public, and investor relations and the need to communicate the effective means being implemented to get the organization back on track.

- *Lack of business support* – Business continuity and disaster recovery is not just an IT issue. All functional business process groups need to be involved in the risk and business impact analysis stages.

(Arata et al. 9).

It's important for these common mistakes to be pointed out up front and to get it in the minds of those involved. This will help reduce the number of mistakes made when developing the BCP.

Chain of Command

Even though there will be more to the BCP and this is just the beginning, it should be stated that in order to activate the BCP, you or a backup are the ONLY ones who can activate such a plan. You will need to be available 24 hours a day and so will your back up by either pager or cell phone. This seems like an obvious piece of the BCP, but it is sometimes overlooked. If you're not available and neither is your back up, who makes the call to activate the BCP?

You and your back up should have a list of local FBI, police, fire, power, and Phone Company as well should they need to be contacted. It would be a good idea to contact these places ahead of time and let them know what you're doing.

Your Role as Coordinator of the BCP

Although many people will be working on the BCP, you'll be the one ultimately responsible for the BCP. If too many people have their hands in the BCP, things can get confusing and will end up hurting the plan rather than helping it. All final changes should be approved by you. Be sure you let those on the BCP Core Team know to come to you with any questions/concerns. We've all been in situations where folks take their concerns to the wrong area. In those cases, you will end up 'fighting fires' instead of paving the way for the BCP Core Team.

Since your organization has never done this before, it's a good idea to have weekly meetings with each area if possible. Don't give your initial presentation to each area and let them go without any guidance. This is new to everyone (including you) so don't be afraid to ask for suggestions or improvements as time goes on.

Odds are you'll get a lot of resistance and hear the statement that was brought up at the beginning of this paper: "We've been doing it this way for years and nothing has ever happened to us." No one likes to change and even with the best presentations and business cases, folks still won't see the benefit of a BCP. If it's coming from someone within a particular area, let their management deal with the situation. If it's the management of a certain area who is reluctant or unhappy with this process, you should try to resolve the issue yourself and if not, escalate the issue. Your main focus should be the BCP.

Conclusion

Once the above steps are put into place, it's a good idea to run it by your senior management one last time. Even though they've given you the approval to develop the BCP, it would be wise to key them in on what you're doing. Also, there will most likely be the need to ask for some extra money to develop the

BCP. The more planning you've done, the more likely they are to give you the money needed.

After all of this takes place, hopefully your organization will be on the right track in developing a BCP. Keep in mind this is only the beginning of the BCP. There is still a lot more work to be done. One thing to remember is there is never an end to the BCP. It should be a living, breathing body of knowledge that is updated and tested. Anytime new technologies are used that are part of the critical infrastructure, it needs to go through the planning stage, and every other stage of the BCP. This may seem like a lot of work, but in the long run, it could mean a lot less work should an outage occur for whatever reason.

Keep in mind there is no 100% full proof plan for business continuity. In this day and age customers want access 24/7 and if you can't provide that, they'll go somewhere else. They will most likely not be interested in why they can't get to your web page and only know that they tried and it didn't work. With the dependence on 24/7 accesses and the ever-changing spectrum of technology, the BCP is more important now than ever before.

I found the quotes below which sums up why anyone who is in business should have some kind of BCP and ultimately why a BCP is necessary:

"'Scenario planning is never a pleasant exercise,' said Chuck Tucker, Gartner EXP vice president and research director. 'However, CEOs owe it to their employees, their families and to shareholders to protect their most valuable assets -- their people -- and to ensure that business can continue even under the most extreme circumstances.'" (taken from http://www.dataquest.com/press_gartner/quickstats/busContinuity.html)

"Business continuity is not about elaborate documents or expensive software; it is about common sense. It is not about pessimism or cynicism; it is about being realistic, sensible and aware." (Saita, 53)

Good luck in the development of your BCP!

References

1. Arata, Michael, et al. Disaster Recovery and Business Continuity Step-by-Step (pgs. 6 – 14). SANS Press, 2002.
2. The SANS Institute. Track 1 – SANS Security Essentials + CISSP CBK 1.2 SANS Security Essentials II: Network Security Overview, The SANS Institute, 2003.
3. Wilson, Belinda. Business Continuity: Never Optional; Now Required. Hewlett-Packard Company. 25 Feb. 2003. http://www.hp.com/execcomm/itjournal/first_qtr_02/continuity.html
4. GuiltMonkey.com. 26 Mar. 2003. GuiltMonkey.com. (1 Apr. 2003). http://www.guiltymonkey.com/gallery/wtc2?&page=2
5. Konner, Cortney. CK. (1 Apr. 2003). http://ckonner.popflux.com/quotes/911.html
6. Solomon, Melissa. "Disaster Eecovery After Sept. 11: Lessons Learned." Computerworld 21 June, 2002. (26 Feb. 2003). http://www.computerworld.com/securitytopics/security/recovery/story/0,10801,72192,00.html
7. Disaster Recovery World. (3 Mar. 2003). http://www.disasterrecoveryworld.com/
8. Kary, Tiffany. "From Ground Zero Up: How 9/11 Changed Disaster Planning." ZDNet 10 Sept. 2002. (5 Mar. 2003). http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2879843,00.html
9. Availability.com. (2 Apr. 2003). http://www.availability.com/elements/information_technology/index.cfm?fuseaction=checklist
10. Disaster Recovery World. (3 Mar. 2003). http://www.security-risk-analysis.com/introduction.htm
11. Gartner Press Room. (7 Apr. 2003). http://www.dataquest.com/press_gartner/quickstats/busContinuity.html
12. "2003 Buyers' Guide." Information Security Magazine. Dec. 2002: 194-195.
13. Saita, Anne (ed). "Philip Jan Rothstein." Information Security Magazine. Nov. 2002: 53.
14. Contingency Planning World. (30 May 2003). http://www.business-continuity-world.com/