Global Information Assurance Certification Paper

Business Continuity: Be Prepared - Be Protected

Libby Foster
October 27, 2003
GIAC Security Essentials, version 1.4b, option 1

Abstract

Forty years ago, a continuity plan was unheard of. Twenty years ago, a plan was only for the overly paranoid – or so it seemed. In today's environment, a continuity plan is essential. Not only do businesses need them, but so do government agencies, non-profit organizations, learning institutions, hospitals and even civilians. For the convenience of this paper, I will approach the remaining information from a business perspective.

The very survival of a business rests on a well written and tested continuity plan. Factors such as financial stability, business operations and personal safety all rely on a plan to ensure a manageable outcome. Business units like Public Affairs, Media Relations and Human Resources should be included in the plan documentation as well. They may have the important responsibility of presenting a single message to the media and employee family members regarding their company's welfare.

The Culprit

Natural Disaster

There are many events that can evoke a continuity plan in some degree or another. The most common include:

- natural disasters
- fire
- environmental hazards
- acts of violence
- terrorism

The frequency of natural disasters cannot be predicted. However, their occurrences are being felt on a fairly regular basis. Earthquakes, flooding, tornadoes and hurricanes can wreak havoc on unassuming entities at anytime, anyplace.

Lessons Learned

"Hurricane Andrew struck southern Florida in 1992. It brought with it devastation and immense human distress. The residential areas in the affected areas were demolished, leaving people in turmoil and chaos. Businesses in the area that had a continuity plan in place, still found recover difficult due to victims primarily focused on their survival and family members, rightly so. Their jobs and the stability of their employer's companies became unimportant. "This vast regional disaster underscores the responsibility companies have to their employees when developing contingency plans." (www.drj.com/special/andrew.html)

During a situation such as this, a tested plan can help keep confusion and chaos to a manageable level. A stable environment can not be expected, but a pre-existing plan can assist key individuals in making sound decisions in an unstable setting.

"For companies in south Florida, personnel problems were worse. Organizations could not communicate with or even locate many employees. Bell South's first priority after the disaster was finding employees and helping their families recover. By mobilizing corporate emergency resources, Bell South tried to meet the survival needs of its employees, providing food, supplies and crisis trauma counseling." (www.drj.com/special/andrew.html)

Other notable natural disasters include the underground flood of Chicago in 1992, which shut down businesses for weeks. In Southern California, the 1994 earthquake produced devastating results for people and businesses/organizations alike.

Large scale natural disasters large amounts of media coverage. In the midst of all the devastation one thing becomes evident, the need for planning. The media directly shows both individuals and businesses what can happen during a disaster and indirectly raises awareness of the need to prepare for the possibility.

The U.S. Department of Homeland Security provides a web site for civilians to prepare themselves. www.Ready.Gov is an excellent source for individuals to consult and gain an understanding of what is necessary for a personal/family continuity plan. With a personal plan in place, it makes it easier to regroup in a disaster situation, and possibly move on to helping employers or others in need.

Environmental hazards

Environmental hazards include gas plants, railroad tracks and chemical plants. Hazards? These don't present themselves as obvious risks to business operations, but they are. A business's location can affect business operations by it's location to potential hazardous surroundings. Trains can de-rail (sometimes spilling hazardous materials), gas plants can explode and chemical plants can emit toxic fumes. All of these situations could result in an evacuation.

Violence/Terrorist Attacks

Violent acts and terrorist attacks upon businesses and property have been more prevalent in the past decade. These include not only extreme attacks such as those on the World Trade Center in 2001, but also disgruntled employees or groups whose purpose is to do as much damage to their target as possible. This could include industrial espionage – attacks on the business's data center or physical breech of security followed by physical harm to employees or the building.

A plan could be evoked based on the severity of the violence inflicted. At a minimum, employee panic and confusion could result, requiring a structured plan in place to restore order.

Location, Location, Location

As mentioned above, a building location should be very well thought out.

External factors offer many threats as well as benefits. If a business is building a new facility, factors such as fire stations and power sources with redundant power grids should be near-by resources. Another consideration should be the high availability of roads/interstates for the possibility of a mass evacuation. If a business has already permanently located and none of the above mentioned resources are near-by, the business should contact their local agencies and discuss options and try to set a plan in place. This agreement between business and local agencies should be well documented within the businesses continuity plan.

Building characteristics need to be considered too. A plain building facade is the safest option in building design to avoid drawing attention. If the company name is boldly displayed on the building, and it is thought that the company has large amounts of money on hand, it is an invitation for thieves and miscellaneous deviants to target. A plain exterior may detract attention from a possible attack.

Gates and fences provide additional security measures. Inside the building, security guards provide protection as well as provide a visible deterrent to would-be attackers. Additional measures such as mantraps and locked doors are effective at providing layers of security to entrances and secured areas such as data centers.

To Recap…

With all the above mentioned factors in mind, a business can prepare the best plan possible. All things must be taken into consideration, things such as location, environmentally hazardous variables, emergency agencies available and building safeguards. With these factors considered prior to a disaster, a company can then begin creating plans that will prove invaluable in a time of chaos.

Let's Get Busy

Once a business considers issues like: location, local emergency agencies and relocation sites, then it is time to turn their attention inward. It is now time to start planning and creating a continuity infrastructure within their company ranks. This can be a tedious and time consuming task. It is important to keep the final goal in mind. A good continuity unit will present a clear vision, let groups know what is expected of them, and most of all, have an understanding of what they are trying to accomplish. With these tools in hand, they can help lead others to producing plans and procedures to assist their recovery.

Some initial continuity processes should be employed early on, to help determine what areas are to be targeted first. Company awareness campaigns are a successful aid to help employees realize the need for continuity plans, and also heighten interest in a unit or area wanting to jump on the band wagon. One of the primary tools to determine which areas require plans is called a Business

Impact Analysis.

Business Impact Analysis

An important function in the continuity process is the Business Impact Analysis (BIA). A BIA helps identify those areas that can place themselves as a mission critical function that will need to be restored quickly. Not just quickly, but immediately due to business need and profit retention. These are the areas that will be adversely effected if there is any kind of outage ranging from staff shortage due to inclement weather to data center shutdown.

"Planning for business continuity involves assessing the impact of various risks on critical business functions. The first step is to identify those functions that, if rendered inoperable, would bring business operations to a halt. Next, the organization must measure the impact of each risk and the probability of it occurring, prioritizing those risks that are most dire. By accessing the business impact and evaluating the probability of risk, an organization is well placed to choose the most appropriate response." (http://www.infy.com/infocus/Nov2001Edition/business_continuity.html)

The continuity unit should assist support areas with completion of a BIA questionnaire. Questions such as, but not limited to:

- "How many customers would be impacted by an outage of your area greater than "x" hours? (where "X" is defined as an acceptable amount of down time.)
- "Who (what groups) would be impacted in the outage?"

Additional questions relating to system platforms involved; how much time is "acceptable" to be down and how (or if) back-ups are completed. The answers to these questions can determine if an area needs a plan, and if so, it can help to prioritize the importance in order of recovery rank. The top ranked areas are termed mission critical functions.

These critical function areas then can focus on their critical requirements. i.e. what resources are required at a minimum to restore operations. These requirements are part of the work area recovery information. Plan teams can determine their minimal requirements for equipment, people and space needed to ensure operations can be recovered as soon as possible. In extreme situations, it would be better to restore 20 work stations in a unit of 50, to be up and running in a smaller time frame. Work area recover information should be flexible enough to set-up immediately on site or at an alternative location.

Now What?

In the event a building is not available to re-enter after a disaster, an alternative site is required to relocate employees and resume business operations. The ideal location would be a hotsite. This is a predetermined location that is equipped to act as close to the original business setting as

possible. Computer systems are loaded with the correct and up-to-date networks,
platforms and applications. Adequate space is available for employees to man the phones and conduct business operations.

Hotsites are typically provided by an outside vendor who ensures everything is ready to go at a moments notice. Vendors require a defined list of individuals that are authorized to declare a disaster and who may notify the vendor they will be moving into the site. This duty is called Disaster Declaration Authorization (DDA).

The act of declaring and moving into a hotsite can be quite costly. However, it could prove invaluable during critical times resulting in preventing loss of revenue. In some situations, a hotsite is used until an alternate, less expensive location is established and functional. This alternative is usually a cold shell.

A cold shell is another predetermined location that can be available on short notice, but does not have the extensive set-up available upon arrival. The cold shell is selected based on it's ability to fit possible requirements such as space, wiring and convenience of location. Extensive time and effort can be required to get a cold shell up and running to suitable standards.

Relocation with the building or other company "out buildings" is an option too. If the damage caused by disaster is not too extensive, it may be possible for the impacted areas to move to another part of the building to re-establish operations.

Once the recovery locations are identified, the progress can begin on the continuity plans.

The Team

The next logical step is to assemble a continuity team. There are many teams as well as players that range from daily operations to executive that need to be involved.

A continuity focused center (or unit), should be established. Whether it is an individual or a group of individuals, this body needs to be in place to provide focus and direction to the supporting team. This center of focus must be willing to pursue their cause with a passion. They are the force that convinces employees that creating, maintaining and updating their plan is vital to the company's stability. Their message must convey a sense of urgency as well as open knowledge sharing.

The structure of the required teams could look like the following:

1. *Executive Team* – a team of company executives that helps promote awareness and continuity buy-in. Many times this is the team who is solely responsible for evoking the disaster declaration authorization (DDA) at the hotsite.
2. *Business Recovery Coordinator (BRC)* – Individual(s) responsible for acting as the single point of contact for the business masses. Typically, there is a separate BRC for data center operations and

large business areas (i.e. Accounting), if the company is large in scale. The BRC helps test and maintain the plans over time, and serves as a vital liaison between executives and daily operations employees during disaster.

3. *Platform Plan Team Lead* – The individual that acts as the central focus for each supporting team. In the data center, examples of platform plans might include Unix, IBM or web based applications. These leads often are responsible for writing and updating their platform's plans. This individual would work with the BRC for critical updates, testing requirements, etc.
4. *Platform Plan Team* – The team members from each system platform or specific business areas that support their plan. This group is called on to make sure critical operations are performed and services remain functional in times of disaster.

Each of these roles works with one another to ensure their plans are acted upon and that ultimately business operations are restored to the greatest means possible.

The teams should be well trained on their roles and responsibilities and know what is expected of them and other team members. Each team has to know specifically what they are accountable for. This reduces confusion in times of chaos, regarding who does what.

Once team training is complete, company awareness should be kept in the forefront. Message points from all levels of management, including executives, should convey the importance and need for well structured continuity plans. Too often, it is easy for this type of work to get placed at the bottom of the pile of daily business requirements. With clear objectives coming from all levels, employees can understand the importance of this kind of work.

Once a working set of full plans are established, they should be tested regularly and updated when discrepancies or gaps are found. Testing should occur multiple times a year. Maintenance of the plans is essential to make sure operational and contact information is accurate and up to date.

The continuity unit and/or the Business Recovery Coordinator should be involved in the plan testing to remain informed, to identify potential conflicts and provide guidance.

Testing 1, 2, 3….

"The measure of success is not whether you have a tough problem to deal with, but whether it is the same problem you had last year." - John Foster Dulles (http://www.cyber-nation.com/victory/quotations/subjects/quotes_success.html)

Testing plans help to ensure plans are up to date and contain accurate information. Scheduled testing also helps alleviate chronic problems that persist, but never are addressed. An executed test can bring the proper attention to reoccurring problems.

There are several different levels of test, they include but are not limited to:

- Tabletop
- Functional
- Full-Scale

A tabletop test is a planned exercise. It is conducted in an casual format where thoughts and ideas are exchanged and sometimes gaps are identified. The most effective method in this level of test is brainstorming.

It typically takes anywhere from one to three months to plan this type of test. The
Test itself could be divided into the following timetable:

"15 minutes – briefing
90 minutes to 2 hours – plan run through
30 to 45 minutes – debriefing

If time permits, plan on 60 minutes to go back into the plan to do corrections on the spot." (CPM 2002 Proceedings)

A functional test is more large scale than a table top test. It includes multiple plans and teams. The simulated impact is multi-platform and therefore requires a large collaborative effort. Planning time prior to the test could be as much as three months.

A full-scale test is as close to real-life as possible. This test involves a larger budget as several teams are affected and try to coincide their plans. If a hotsite is available, teams most likely will be transported to that location and test on the equipment and resources at that site. "Planning time for a full-scale test could be at least four months minimum." (CPM 2002 Proceedings)

Each type of test should begin with a clear objective. The participants should understand the objectives and their roles. Factors may emerge from the test that bring questions, but do not fall within the limits of the objectives. It is important to instruct the participants what is and what is not within scope.

Change is inevitable. It is possible that in time plans may change drastically if not dissolve completely. Testing on a regular basis helps to keep these changes in check. It may also be appropriate to confirm plans to create a more dynamic solution. Plans with similar platform processes and procedures make good candidates for a combined plan.

Continuity as a Money Maker

Many vendors now offer continuity "devices". Products ranging from data center smoke/water detectors that immediately reroute to an off-site back up machine, to consulting services and continuity plan software. Big name manufacturers such as IBM, Dell and Hewlett Packard all offer continuity based services of one or more type. The need for a good plan can no longer be overlooked.

Factors like heat, humidity, smoke and lack of air flow can present themselves, but don't always appear as part of a disaster. They can however, cause disastrous results if they are not considered a possibility. Dell's Business

Continuity division reminds businesses of the importance of a plan in this way, "What's at stake?

- Retain customers by avoiding disruptions
- Ensure contact between government agencies
- Assert management and control through crisis
- Maintain employee compensation and supplier revenue streams
- Comply with regulatory requirements
- Keep educational institutions in operation"

(http://www1.us.dell.com/content/topics/global.aspx/solutions/en/business_cont?c=us&cs=555&l=en&s=biz)

From the exercise of the once thought overly paranoid, to the requirement of any business with a goal to endure, continuity has shown up in the forefront and brought with it a market of products and services that will assist businesses with their planning.

Global scale vs. homeland operations

Planning for the unforeseen future is a challenge all businesses face. In today's global economy, the need for continuity protection is multi-layered. An organization that conducts business in multiple countries may potentially face more threats than a national organization. Economic and political factors have played a large part in recent acts of terrorism at home and abroad. Organizations with global offices and/or global business associates (such as suppliers), should realize continuity plans should be specialized for each region. General cultural practices, legislation and environmental policies differ greatly from one nation to another and should be researched in depth while creating a continuity plan. Differences in cultural beliefs could drastically change the procedures within the same plan, depending on the national location.

For example, let's theorize that some time in the future, the United States' shortage on readily attainable natural gas causes many American businesses in that industry to begin importing natural gas from Australia. A continuity plan for the American businesses would need to include back-up plans for supplier problems. If the Australian supplier goes out of business, succumbs to the potential hazards of operating a natural gas plant (i.e. explosion, or mass evacuation due to a leak), or even becomes the subject of a terrorist attack, this would mean trouble for the American importer. Alternate means of supply should be in place in case the primary supplier is not able to fulfill their contract.

When beginning a multi-national negotiation with a supplier, it would be well advised to ensure they have a continuity plan themselves. This would provide some insurance that processes are in place to enable the recovery of business operations within a reasonable time frame.

On the other hand, a local or national company that only practices business within its nation's borders would not have to have quite a complex continuity plan. Generally staffing, budget and research & development are among the most common areas typically included in an organization's planning

cycles. Continuity should be one of the high priority areas too. Without it, an organization is putting their very existence at risk. While it might be difficult to justify continuity in the budget due to its theoretical basis, it would be much more difficult to justify why a plan was not in place during a time when it was needed. "According to Mainframe Week, IBM and the Wall Street Journal's research on major disasters, the statistics paint a bleak picture for those firms that do not have a solid Disaster Recovery Plan. Companies experiencing 2-5 days of downtime in these events that did not have a Disaster Recovery Plan had the following results:

- 5% went bankrupt immediately
- 40% Closed their doors within 2 years
- Of the 35% remaining, virtually none were still around 5 years after the disasters" (http://www.blackchambernj.com/technology/disasterrecovery.htm)

Summary

It makes good sense to use a continuity plan no matter what type of organization is involved, physical and economic survival can depend on it.

List of References

1. Arnold, Richard L. "Special Report Hurricane Andrew The Human Side of Hurricane Recovery." Disaster Recovery Journal. 2001
URL: www.drj.com/special/andrew.html

2. "Business Continuity How do I protect my business from natural or catastrophic disasters?" Dell USA Medium & Large Business. 2003
URL:
http://www1.us.dell.com/content/topics/global.aspx/solutions/en/business_cont?c=us&cs=555&l=en&s=biz

3. "Disaster Recovery Don't Risk Losing It All". The Black Chamber of Commerce of Northern New Jersey. 2001 URL:
http://www.blackchambernj.com/technology/disasterrecovery.htm

4. Kumar, Praveen & Muthukrishnan, Krithika. "Business Continuity Planning for the Information Age." InfosysTechnologies Ltd. November 2001. URL:
http://www.infy.com/infocus/Nov2001Edition/business_continuity.html

5. Phelps, Regina. 2002. "Everything You Need To Know To Conduct Effective Emergency Exercises". Symposium conducted at CPM 2002 Proceedings in New Orleans, Louisiana.

6. U.S. Department of Homeland Security. 24 October 2003. URL:
http://www.Ready.gov

Last Updated: July 27th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event