GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Business Continuity Planning

There are many things beyond the control of a corporation which can cause a disruption in a business' ability to provide products and services. Natural disasters, employee mistakes, system failures, data corruption, deliberate information systems attack, terrorism even loss of life of key personal is a viable reasons to plan for when considering Business Continuity. Protecting your business from these threats is just the first step in Security Management but what about after a disaster occurs? Business Continuity Planning is the next step and I believe works hand-in-hand with corporate security. Here are a few facts to consider when designing your Business Continuity Plan.

- Computer down time costs US businesses $4 billion a year, primarily through lost revenue.
- 20% of all small to medium size businesses suffer a major disaster every five years
- Criminals now choose electronic methods of harming business more than any other
- 60% of the business in the World Trade Center were out of business within two years of the terrorist bombing of 1993 because they did not have business continuity plans.
- Complete numbers have not been gathered about the September 11, 2001 terrorist attacks in the World Trade Center but companies now have to think about the lose of life of key employees as well.

Business Continuity is not to be confused with Disaster Recovery. Disaster Recovery focuses on a single system and what is required to get that system back into a functional state. Business continuity incorporates Disaster Recovery and takes a few giant steps forward. Business Continuity Planning (BCP) is concerned with the business as a whole from security for employees and computing systems to network connections, phone systems, environmental systems, etc. BCP hopes to answer the following questions and more:

- How do I stay in contact with my customers?
- How do I processes customers orders or supply the service they have contracted?
- What are my critical systems and procedures?
- How do I protect my employees?
- How do I protect my data?
- How do I replace critical systems or procedures if they fail?
- How much will replacement of critical systems or processes cost?
- Do I need and alternate site?
- If I do need and alternate site, what type of security is supplied? what do I need to supply? (firewalls, security personnel, procedures)
- Is it financially feasible to replace all computerized functions or do I need a manual process in the interim?
- Can my customer wait for a product they usually received in a few days?
- How do I pay my creditors?
- Am I insured for such an event?
- Will I still be in business if I cannot answer any of the above?

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Business Continuity does not concern itself with long term business risk. Long term business risk refers to changing markets or changes in competitiveness. These are things management should be prepared to handle. It does not address risk associated with exploiting new opportunities nor does it plan for low impact problems unless they turn into major problems. Low impact problems should be resolved via service level agreements and problem management processes.

As Dan Carson and Brian Zawada wrote in their paper "Business Continuity Planning and the Ten Most Common Pitfalls to avoid in the New Economy" there are 4 key phases that a Business Continuity Planning Process should contain. They are as follows:

- Discovery and Planning
- Risk, Business and Cost Analysis
- Plan Development and Maintenance
- Plan Validation, Training and Approval

Discovery and Planning.

Goal

- A detailed project plan
- Documented business processes
- A database of resource and asset inventories related to recovery
- A listing of insurance and other policies related to recovery

Discovery and planning phase should define the scope of the BCP project. During discussions with key management representatives from all business units and IT professionals, expectations and goals of the project should be defined. At this point of the process you should go over your business with a fine toothed comb. Collect vendor names and numbers, conduct inventories, collect processes and any previous BCP or recovery plans. Remember internal processes and data is confidential and should not be shared with individuals or groups who do not have the need to know. This includes internal as well as external entities. The discovery and planning phase should allow you to walk away with a time line for the project. Hopefully you will get an idea of what state you are currently in and where you hope to be.

The time line should address the next 3 to five years. Be as specific as you can for the first 2 years and, if need be, generalize as you go further. Remember, as new technologies enter your business your timeline will need to reflect those changes as well. Keep in mind that the BCP process will need to be cyclical. Although it's easier said than done, try to keep politics out of this process. During the initial stages of BCP planning, it is very important to remember that the ability to keep the business in an economically viable state is the most important reason you are creating a Business Continuity Plan. Managers and technicians usually believe the assets they are responsible for are just as important as any other system. While the assets they manage do server a purpose in the grand scheme

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

of things, there are assets and systems that are most critical to the business and those assets and systems are what needs to be identified in the next section.

Risk, Business and Cost Analysis

Goal

- Risk assessment
- Business impact analysis
- Cost benefit analysis

The Risk, Business and Cost Analysis phase consists of identifying the types of risks your business may encounter. Risks to be identified can be environmental, business, security and industry type risks. Examples of environmental risks are risks such as building in a flood zone, or in areas affected by hurricanes or tornadoes. Business risks are risks such as contracting a critical service through a company which could go out of business in the future. Security risks such as data centers without the ability to lock out or screen the individuals who enter it. Industry risks such as the depletion a of a vital resource causing a shortage of processors. The risk analysis could shine the light on problems which can be fixed immediately, while others may take some forethought to resolve.

The Business impact analysis determines what the potential losses could be to your company if the company actually experienced the disasters predicted in the risk analysis. This analysis should take time frames into account. Can the company survive for days or only hours with a specific service unavailable.

And finally, the cost benefit analysis. After determining the business impact, it's time to determine what it is going to cost to recreate those processes or systems if a disaster occurs. The costs of replacing processes or systems should be weighed against doing nothing.

Plan Development and Maintenance

Goal

- Recovery strategy recommendations
- Business continuity plan, including procedures for emergency response, business resumption and business restoration
- Recovery team procedures
- Plan change control and maintenance

Plan development and maintenance is used to plan recovery strategies, develop the BCP plan, determine who will be part of the recovery team and how to keep the plan current to meet business needs.

These sessions should include representatives from the following groups:

- a full time planner

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Datacenter operations
- Network – wide and local area data communications
- Help Desk
- Security Manager
- Client/server computing
- Corporate, cross department and business application support
- Lines of business and end-user application support
- Systems and database programming
- Internal audit

Recovery strategies should consist of brain storming sessions. Use the risk analysis you created earlier to give you something to focus on. For instance, if your financial system has a hardware problem, what do you do? If it is not the end of a pay cycle you may have time to wait for parts and recover from tape. If it is the end of a pay cycle, do you restore to a different server? Do you use other solutions such as a SAN to mirror your data? How would incremental backups help or hurt your restore times? This will be a very time consuming process as each conceivable risk should be addressed so the proper decision can be made.

The BCP plan should address emergency response, business resumption and business restoration. This plan should be distributed to all personal who will be part of the response team. The plan should also be on alternative media (on CDROM, on paper) and in alternative locations (in the company vault, at employees homes, on file).

If the plan is not up-to-date for your business needs it is not going to be very valuable in a time of need. Procedure must be put into place which address maintaining the BCP plan. As new technologies are introduced into the company you should identify the risks to the new technology, the costs of those risks to the business and the cost of replacing the technology. You should also decide where this new technology fits into the your current plan. Will take the place of an older technology or will it be added to your BCP?

<u>Plan Validation, Training and Approval</u>

Goal

- Documented test plans and evaluation criteria
- Documented test results
- Trained BCP personnel
- Structured training program and materials
- Senior Management approval

Validation of the plan is crucial. If, after going through all of the steps above, you feel that you have prepared yourself for any contingency, think again. Although you will be able to prepare yourself for most disasters, eventually, you will experience something you couldn't imagine. Only by testing your plan for the risks you can identify, will you be ready to handle the risks you couldn't identify. Testing is also a great way to discover

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

flaws in your thinking, identify inappropriate assumptions and identify where your employees need more training.

The BCP exercise should be based on a realistic set of goals for each exercise. Document those test goals and the results of the exercise. The documentation can be used for updating the recovery procedures, to keep an accurate time line of the training session and to be used in a Post Mortem to determine if errors that were encountered were due to system errors, planning errors or experience levels.

In my experience you can try to make a document as idiot proof as possible but unless all of the employees expected to use it have the exact same background and experience there will always be questions and uncertainties. Practice is the only way to give your employees a level of confidence in the plan and in their abilities to think on their feet when needed.

One item I feel is very important at this point, is to let individuals involved in planning and testing the BCP process know that a failure in testing is not a failed exercise. After all, the testing phase is required to identify flaws in your thinking, indicate assumptions which aren't true or perhaps indicate where employees require more training or a better understanding as to their roll in the BCP process. The only unsuccessful BCP exercise is one that, based on assumption that you are ready for anything, is never completed.

Senior Management should view the results of the BCP exercise and make recommendations appropriately. If they are satisfied with the results perhaps no recommendations are necessary. I have never been involved in a BCP exercise that hasn't yielded changes to the current plan.

Conclusion

In a market economy, it can be difficult for management to justify the cost of Business Continuity Planning. But failure to achieve the organization's stated minimum acceptable level of business will mean that severe damage to that business' future economic resolve could result. With all emphasis on the bottom line and on earnings per share, Business Continuity Planning looks like a cost with no return. No return, that is, unless a disaster occurs. BCP is an insurance policy against disasters seen and unseen. It prepares employees for such events by training them to handle almost any conceivable event. It forces employees and management to consider how critical pieces of the organization can effect the company as a whole.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

References

Dan (ABCP) and Zawada Brian(CBCP), *Business Continuity Planning and the Ten Most Common Pitfalls to Avoid in the New Economy* Carson
http://www.aametrony.com/downloads/whitepapers/BCP.doc

Keeling, Chris and O'Reilly, Steve, *Business Continuity in the E-Commerce Environment*
http://www.insight.co.uk/pdf_files/bcm_in_ecommerce.pdf

Unknown Author, *Business Continuity*
http://storage.tracenet.net/cgi-bin/articals/view.asp?id=139

Marvell Simon,*Business Continuity Management in the 21st Century*
http://www.insight.co.uk/pdf_files/bcm21.pdf

Compaq Document, Author Unknown, *Disaster Tolerance, The Technology of Business Continuity*
www.techguide.com

Philip Jan Rothstein ,*The Politics of Recovery Testing*
http://www.icsalabs.com/html/library/whitepapers/Politics_Recovery_Testing.pdf

Kelvin Lack, *Turnbull the Implications for Business Continuity and Information Security*
http://www.insight.co.uk/pdf_files/turnbull.pdf

© SANS Institute 2000 - 2002, Author retains full rights.

Last Updated: April 27th, 2017

Upcoming Training

Click Here to
{Get CERTIFIED!}

SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
Community SANS Philadelphia SEC401	Philadelphia, PA	Jun 19, 2017 - Jun 24, 2017	Community SANS
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS