Beyond Buy-In: The Case for Executive Level Involvement in Developing a Business Continuity Plan

Anne Humphrey

Beyond Buy-In: The Case for Executive Level Involvement in Developing a Business Continuity Plan

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4c

Option 1 - Research on Topics
in Information Security

Submitted by: Anne Humphrey, March 9, 2005
Location: Washington, DC

The development of a robust business continuity plan is an essential activity for any organization. Too often companies limit executive level participation to approval and funding roles. It is becoming increasingly apparent that the nature of the business continuity plan development process and regulatory requirements demand a more integrated participation level by those responsible for leading an organization.

Table of Contents

Abstract/Summary

The development of a robust business continuity plan is an essential activity for any organization. Too often companies limit executive level participation to approval and funding roles. It is becoming increasingly apparent that the nature of the business continuity plan development process and regulatory requirements demand a more integrated participation level by those responsible for leading an organization.

Introduction

A consistent theme in articles on business continuity plan development is the need to create buy-in at the upper management level. As recognition increases about the key role a well developed, maintained and exercised Business Continuity Plan plays in the make-up of a robust company or organization, it is critical to recognize that the role of upper management should evolve beyond buy-in. The buy-in level of support implies a willingness to fund the enterprise, hire the appropriate staff and delegate responsibility. Recent studies have demonstrated increased levels of funding for business continuity related efforts. "According to US research firm Meta Group, companies spent just 3.2 percent of their IT budgets on security (employee education, business continuity and disaster recovery) in 2001. Last year, the outlay was more like 8.2 percent- a dramatic increase." (Goff, 1) Increased commitment of financial resources is just one reason to encourage increased upper management involvement. There are also clear calls for increased involvement from leaders in the government. On December 21, 2004 "the director-general of England's MI5 national security agency told UK businesses that the most effective thing they can do to protect themselves against terrorism is to develop a simple but effective continuity plan and to ensure that business continuity plans are considered at a board level, and not 'left to specialists'." ("Head of UK's MI5 Recommends Investing in Business Continuity" 1).

Increased spending and calls for corporate leadership involvement are significant reasons alone, but a closer look at the development of a Business

Continuity Plan also argues for this level of integration in the process. The foundation of the Business Continuity Plan itself is highly dependent on gathering reliable data and a clear vision of the company's priorities and obligations. This paper examines the need for and impact of this involvement during two critical stages of the BCP development- the Business Impact Analysis and the Developing Business Continuity Management Strategies phase ("Professional Practices for Business Continuity Planners"). The success of a Business Continuity Plan and therefore the ability of an enterprise to remain resilient in challenging situations will become increasingly dependent on the integrated involvement of the corporate leadership throughout the process.

Business Impact Analysis

The professional practices guidebook for business continuity planners developed jointly by two of the leading organizations in the field, DRI International and the Business Continuity Institute (BCI) describes the Business Impact Analysis (BIA) as a phase to "identify the impacts resulting from disruptions and disaster scenarios that can affect the organization and techniques that can be used to quantify and qualify such impacts." The BIA further enables the business continuity planner to "establish critical functions, their recovery priorities, and interdependencies so that recovery time objective(s) and recovery point objective(s) can be set." ("Professional Practices for Business Continuity Planners").

An analogy may be made between the Business Impact Analysis process and the dissection a 1st year medical student performs on a cadaver. Just as each of the different systems that make up the human being is individually separated and studied for its unique qualities and interdependencies in the gross anatomy lab, so to do the individuals performing a Business Impact Analysis need to analyze the anatomy of a business. While the medical student is attempting to gain a better understanding of the patients s/he will be treating, the business continuity planner is seeking to understand the enterprise s/he is engaged in assuring. To continue the analogy, a medical student is not asked to engage in the dissection without guidance, nor should the business continuity planner be asked to understand the unique nature of a company or an organization without significant guidance and involvement from corporate leadership.

The BIA process may be broken into the following stages: project planning, data collection, data analysis, reporting of the findings and approval for the next stage ("DRP 501 Business Continuity Planning Review", 53). The project planning stage is similar to most project plans in that it lays out the scope and objectives of the activity. Most business continuity planners rely on a combination of interviews and questionnaires to gather data about the various business functions. Additionally, the planner will gather any reference documents that exist within an organization: mission statements, organizational charts,

employee manuals etc. ("DRP 501 Business Continuity Planning Review", 61).

During the data collection phase of the Business Impact Analysis, questions like "What are the critical business functions? What is the cost per hour if the organization loses that function? Is this an org that relies heavily on e-commerce? What is it current state of readiness? How quickly and in what hierarchy must systems be restored?" (Chalfant, 2). The answers to these types of questions will further assist the planner(s) ability to "identify the organization's mandate and critical services or products; rank the order of priority of services or products for continuous delivery or rapid recovery; and identify internal and external impacts of disruptions" ("A Guide to Business Continuity Planning", 3). While it is generally considered a business continuity best practice to engage the front-line managers n the data collection process, it is also essential to have equally detailed conversations with corporate leadership. The current and desired future state of an enterprise is uniquely viewed and articulated by those with the ultimate responsibility for leading the organization to that goal.

The analysis phase of the Business Impact Analysis process addresses both quantitative and qualitative issues within the organization and is essential to capture both. Quantitative measures are often numbers or statistics that are easily captured and understood such as the loss of sales over a specific period of time. However, qualitative issues such as loss of customer confidence are harder to measure but are equally damaging to a company's on-going viability.

The reporting of findings is fairly typical of any type of data collection and analysis with one of the primary objectives being the establishment of Recovery Time Objective or RTO for the various business functions or application systems. The Recovery Time Objective is one of the key building blocks in the decision-making process that occurs during the selection of a business continuity strategy. The Recovery Time Objective (RTO) may be defined as "the time within which business functions or application systems must be restored to acceptable levels of operational capability to minimize the impact of an outage" ("DRP 501 Business Continuity Planning Review", 52). One suggested best practice to consider while determining the Recovery Time Objective (RTO) is to consider the question within the context of a peak period of activity within the organization. Establishing what is the longest acceptable outage for the most demanding performance period will ensure that the Business Continuity Plan will accommodate all timeframes.

While it is essential to have an experienced business continuity planning professional guide the process of the BIA, a truly successful BIA will best result from an integrated participation from the highest levels of the enterprise as well as the front line managers. The vision and direction for the organization that comes from the highest levels of leadership should guide the creation of the priorities for business continuity efforts. Who better to help establish and define the key relationships, products and systems than the individuals responsible for

guiding the enterprise as a whole? A typical failing of corporate leadership in the business continuity planning process has been to equate BCP with the continuity of IT infrastructure like data centers. As noted by Joe McKendrick in a recent article on database recovery "much of the planning- and more importantly- budgeting behind BR and DC is coming from parts of the company beyond the immediate reach of the data center. However, unless an actual emergency jolts executives out of their complacency, such efforts can be either under-prioritized, underfunded, or- at the opposite extreme- overdone with expensive duplicate systems. "(McKendrick, 1). A more complete integration of the leadership into the BIA process will enable a more reliable and timely development of the RTO and other key outcomes that are the essential building blocks of the Business Continuity Plan.

Developing Business Continuity Strategies

The professional practices guidebook describes the Developing Business Continuity Strategies subject area as the place where an organization will "determine and guide the selection of alternative business recovery operating strategies for recovery of business and information technologies within the recovery time objective, while maintaining the organization's critical functions" ("Professional Practices for Business Continuity Professionals"). The data that is needed to determine what recovery strategies are most appropriate for a given business's unique operating reality is determined in the BIA. This phase explores a number of options ranging from do nothing to a hardened fail over site.

Each option has its own advantages and disadvantages in terms of cost, availability, time to implement and security. Below are brief descriptions of each of the main options considered. ("DRP 501 Business Continuity Planning Review", 10-13)

Services Degradation: as implied by the title, this strategy accepts a decrease in performance as part of its recovery strategy. This strategy is one that may be considered when the Recovery Time Objective is lengthy or when the cost of other options would be overly burdensome to the organization's ability to perform at acceptable levels during normal operating periods. This strategy may be used in combination with other strategies.

Internal Recovery: is an option that may be pursued when an organization has sufficient resources to redistribute business functions throughout other locations.

Duplicate Sites, distributed: When a company strategically duplicates key business functions and processes throughout its geographic locations it permits this recovery strategy that, while expensive, is independent of external providers and enables increased levels of customization, security and is available for test an exercise activities. One challenge that is often seen in these arrangements is the requirement to maintain consistency between the sites in equipment and processes.

Cold site: a cold site is typically a room with the basic infrastructure available- e.g. phone and data lines can be set up when needed. All computers, furniture, other resources required to resume operations will need to be installed as part of the activation. A cold site is one of the least expensive options and is often used as part of a phased approach or for a business operation with a long RTO. It allows for a customized response to the situation being responded to but is unable to be effectively used for any test and exercise of the business continuity plan.

Hot site: is characterized by its ability to accommodate a short RTO through its high state of readiness. All infrastructure and equipment needed to continue business operations are available. As expected, this is one of the most expensive options but enables the quick resumption of business operations and is also an excellent resource for testing and exercising the Business Continuity Plan. Hot sites may be set up and controlled by the company anticipating the future need or may be leased through commercial vendors. The shared arrangements of a commercial vendor allow for significant cost savings while maximizing readiness but also have some shortfalls. One risk associated with commercial vendors is the impact a regional incident might have on their ability to deliver on their contract. “Consider how pressed hot-site facilities can be in the event of disaster such as the widespread power outage in the 1990s that sent scores of companies to their hot-site vendors. With thousands of displaced employees needing alternative sites to work from, hot site vendors turned data center space into workspace for customers. Productivity plummeted as workers tried to deal with the noise of cramped quarters and the chill of working in a facility kept intentionally cool for computers.” (Chalfont, 3) Additional security concerns are also raised by potential competitors sharing space and equipment.

Warm Site: as indicated by the term, a warm site resides between cold and hot sites on the level of infrastructure and equipment provided. It enables a company to transfer data from the main location and bring up operations- typically in about 24 hours. Warm sites also fall between the two extremes of hot and cold sites in terms of cost. A company with a RTO that is longer than a few hours might find this a cost effective option.

Mobile Site: an additional option to an alternate site includes mobile sites. Mobile sites are essentially trailers loaded with servers, computers, communications equipment and other necessities that can be rolled to whatever

location is required. In some cases, companies have utilized a mobile site next to a hot site for increased capability. "Until the recent train bombing in Spain, a mobile site next to a hot-site might have qualified as disaster-recovery overkill. But such a view ignores the Herculean coordination necessary to run a transcontinental railroad. 'If we can't throw switches…we're out of business'".: (Goff, 1)

Hardened Site: companies and industries that have been warned of increased risk for being terrorist targets or for other acts of malicious damage may also employ what is know as a hardened site. "for security reasons, some organizations employ hardened alternate sites. Hardened sites contain security features that minimize disruptions. Hardened sites may have alternate power supplies; back-up generation capability; high levels of physical security; and protection from electronic surveillance or intrusion" ("A Guide to Business Continuity Planning" 5). The explicit threat to the US financial industry has resulted in many companies implementing these types of measures. In testimony before Congress this past fall, companies operating under the raised terrorist threat level in New York, New Jersey and Washington presented the measures they have put in place to increase their level of security. "In addition to mandating that a certain percentage of personnel work off-site at any given time, the NYSE has worked with New York City officials to reroute bus traffic around its datacenters, hired a 24-hour New York Police Department security detail for all datacenters and deployed a geographically diverse fibre-optic routing backbone" (Verton 1). These additional security measures are also being put in place at remote facilities that serve as back-ups.

Fail-over site: the most expensive option that is capable of almost instantaneous resumption is the fail-over site. If a primary system fails, these sites have the capability to automatically switch operations to their standby database, server or network. These are typically employed by businesses that are reliant on 24-7 customer accessibility and high volume like website hosts (Goff 4).

Other options that may be considered include: business recovery centers, outsourcing, quick ship and reciprocal arrangements ("DRP 501 Business Continuity Planning Review" 11). As with the previously detailed strategies, each of these has advantages and disadvantages. A business recovery center may not require as much financial commitment from an organization as a commercial hot site, but may have difficulty providing the level of service required at the time needed, or may be impacted by the same event. One recent example is the massive power outage that affected most of the east coast and Canada in the summer of 2003. "Many businesses discovered that their remote sites weren't remote enough. "It's all right to have a back-up center…but if you're in the same power grid, it doesn't do you any good" (Goff 3)

A quick-ship arrangement for key materials may be a cost-saving measure that is especially useful when implemented in conjunction with another strategy like a warm site, but may be less than what is needed if an organization is fumbling for a location to work from.

Reciprocal arrangement may work well when developed between organizations that have are complementary, have a history of collaboration and do not compete directly with each other. However, ensuring that each organization maintains levels of compatibility in IT infrastructure and other key areas as time passes will become increasingly challenging.

It is clear that each individual company or organization requires its own unique strategy. There are no perfect, one size fits all solutions, even within industries or for comparably sized companies. "The fact of the matter is that both external and internal recovery solutions are viable options. A particular organization can only decide which is right for it based on a balanced evaluation in context of the organization's mission-critical requirements. In some cases, the great cost of establishing internal recovery facilities will be justified by increased control over availability and customer satisfaction. In other instances, an organization's requirements and expectations may not justify the cost of an internal recovery location." (Croy 3) This "balanced evaluation" can only be arrived at through involvement of all key players, especially executive leadership and those with ultimate responsibility for an organization, during both the Business Impact Analysis phase and the Developing Recovery Strategies phase.

Regulatory Drivers

In addition to the reasons that exist due to the nature of the Business Continuity Plan development, there are increasing regulatory pressures that drive increased levels of executive involvement in all aspects of business continuity. "Executives are also becoming more directly involved because of government regulations such as Gramm-Leach-Bliley, Sarbanes-Oxley, and HIPAA that hold them personally and legally liable for business issues including access to critical information, financial controls, customer privacy, and physical security." (Croy 4) This is in addition to other drivers for executive involvement with which they may be more familiar with " such as insurance audits, SEC regulations, and bank covenants, as well as basic fiscal imperatives to protect assets and opportunity costs against business disruptions." (Croy 5)

As executives face increased pressure to account for their company's resilience, there is a disconnect between their perception of their ability to deliver and results from some of the latest studies, specifically the Harris Poll. "While C-

suite executives at Fortune 1000 companies tout their ability to access critical information when faced with power outages, hackers, viruses, and natural disasters, study results show they are not being completely objective in their evaluation" (Palermo 1). Many executives recognize the public relations and marketing benefits of touting their preparedness, but actually taking the necessary steps in terms of both financial commitment and personal commitment and involvement in ensuring that preparedness is lagging. "Disaster preparation is not "top of mind" in the boardroom because more than half (56 percent) of the respondents said their company discusses policies regarding access to business critical information either not very often or not at all. Without the constant reminder of a large-scale disaster, it seems top-level executives aren't paying enough attention to this matter." (Palermo 3).

This will become increasingly apparent as legislation requires audits that assess a company's Business Continuity Plan and overall preparedness. As noted in the recent article in Disaster Recovery Journal, "compliance is a problem because nearly one-in-four (22 percent) respondents said their company did not meet regulatory requirements for business continuity, information security, and/or electronic records retention" (Palermo 2). These external assessments are also increasingly valuable as "Perception is not reality because executives graded themselves with a B, while substantial deficiencies exist in their disaster preparation practices" (Palermo 2).

Executives who commit themselves and their fellow leaders to the business continuity plan development process stand to gain a competitive advantage. Their peers may well fall behind as they are impacted by the regulatory non-compliance during non-crisis periods in addition to being less well-prepared to respond effectively during critical crisis periods.

Conclusion

While essential roles are played during all phases of the Business Continuity Plan, one of the most obvious being the role played by emergency personnel during the immediate response to an incident, much of the ability for a successful response is determined in some of the earliest phases of the business continuity plan development lifecycle. It is in these early phases that corporate leadership must play an integrated and comprehensive role in the process. "Deciding how much loss it can accept must be made by executive management based on a full understanding of the organization's interdependencies and all the potential impacts of a loss." (Croy 5)

The ideal end state for a business continuity plan is one that permits on-going functionality at an acceptable level, even when impede by challenging circumstances. As stated in Canada's Guide to Business Continuity Planning, "a business continuity plan enables critical services to be continually delivered to

clients. Instead of focusing on resuming a business after critical operations have ceased, or recovering after a disaster, a business continuity plan endeavors to ensure that critical operations continue to be available" ("A Guide to Business Continuity Planning" 1).

The business continuity professional may be able to demonstrate the need for comprehensive executive involvement through proven best practices like tabletop exercises. However, it will ultimately be the responsibility of the leadership of any organization to fully embrace their responsibility to play a key and integrated role in the development of business continuity plans.

References

Chalfont, Randy. "Be Prepared: Finding the right business continuity solution for your data." Unisys World. Volume March 2003. 1-5. 5 March. 2005. http://www.unisysworld.com/monthly/2003/03/prepared.shtml

Croy, Michael. "Landing On Your Feet Being Prepared in the 21st Century." Disaster Recovery Journal Volume 18. Issue 1 (Winter 2005): 1-7. 7 March. 2005 http://www.drj.com/articles/win05/1801-01.html

DRI International. DRP-501 Business Continuity Planning Review. Falls Church, VA. 2003.

DRI International and Business Continuity Planning Institute (BCI). Professional Practices For Business Continuity Planners. Falls Church, VA. 2003.

Goff, John. "In Case of Emergency." CFO Asia. June 2004. http://www.cfoasia.com/archives/200406_06.htm

"Head of UK's MI5 Recommends Investing in Business Continuity." Contingency Planning Management Group. Dec. 21, 2004. 1-2. 5 March. 2005. http://www.contingencyplanning.com/news/22.aspx?ebid=312

McKendrick, Joel. "Dual Data Centers Accelerate Recovery Strategies." Database Trends and Applications. Oct. 2004. 1-4. 5 March. 2005. http://www.dbta.com/in-depth/oct04/mckendrick.html

Office of Critical Infrastructure Protection and Emergency Preparedness, Canada. A Guide to Business Continuity Planning. Last modified 2/3/2005. 5 March. 2005. http://www.ocipep.gc.ca/info_pro/self_help_ad/general/busi_cont_e.asp

Palermo, David. "The Crisis Facing American Business." Disaster Recovery Journal Volume 18. Issue 1 (Winter 2005): 1-4. 7 March. 2005 http://www.drj.com/articles/win05/1801-01.html

Verton, Dan. Computer Weekly. Sept. 9, 2004. 1-2. 5 March. 2005. http://www.computerweekly.com/articles/article.asp?liArticleID=133190&liArticleTypeID-20&liCategoryID=2&liChannelID=22&liFlavourID=1&sSearch=&nPage=1

Last Updated: October 31st, 2020

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Sydney 2020	**Sydney, AU**	**Nov 02, 2020 - Nov 14, 2020**	**Live Event**
SANS Secure Thailand	**Bangkok, TH**	**Nov 09, 2020 - Nov 14, 2020**	**Live Event**
APAC ICS Summit & Training 2020	**Singapore, SG**	**Nov 13, 2020 - Nov 28, 2020**	**Live Event**
SANS Community CTF	**,**	**Nov 19, 2020 - Nov 20, 2020**	**Self Paced**
SANS Local: Oslo November 2020	**Oslo, NO**	**Nov 23, 2020 - Nov 28, 2020**	**Live Event**
SANS OnDemand	**OnlineUS**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**