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: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

BUSINESS CONTINUITY PLANNING: AN OUTLINE WITH ANNOTATION

Introduction

Managing a secure system not only means keeping the bad guys out, it means access to the information is possible under any circumstances, i.e. that it is available to use, and that a disruption in the business environment does not mean a disruption in the provision of information services. Ensuring the continuity of information services provision, under physically disruptive conditions, is as crucial a concern for security professionals as preventing or responding to hack attacks, viruses, worms, and other malicious attempts to destroy IT resources. It means, simply, making sure that an organization is prepared to continue to do business no matter what the threat, and no matter what the physical environment or conditions.

Many, if not most, organizations have Disaster Recovery (DR) plans in place, whether they have outsourced the function or are prepared to provide it for themselves. But discontinuity can occur under conditions that do not call for an all out DR response. Natural disasters such as earthquakes, floods, hurricanes, or fire can of course result in system shut downs of a significant enough nature to call for DR activation. But they can also result in temporary short term disruptions that if not planned for with the same thoroughness and attention to detail as was given to DR planning, can mean an equal amount of damage to the business as a whole.

In addition, short term business discontinuity can occur as a result of bomb and bio-terrorism threats, building shutdowns related to compromised employee security, and other disruptions. And, those threats can also take a significant toll on business services if the response to disruption is not planned for in detail.

So, while DR and Business Continuity (BC) management have become almost synonymous in the arena of system security, for the purpose of this paper, I will use DR to refer to long term disruption (e.g. a week or more) and BC to refer to short term disruption (e.g. 24 - 72 hours). And although the distinction is admittedly arbitrary, BC management is much more likely to be useful since a short term disruption is more likely to occur and to occur more often than a total disaster. Therefore, BC planning is at least as critical as DR planning. [1]

Furthermore, DR planning has historically taken a reactive posture (e.g. "If there is an earthquake, and services are significantly disrupted, this is what we will do: …"). BC however, attempts to begin with a proactive stance. It involves taking the necessary initial steps that will enable an organization at least to return critical services to their necessary

© SANS Institute 2000 - 2005 Author retains full rights.

level within hours. It may even preclude their disruption to begin with (e.g. "In order to keep business going in spite of a building evacuation, this is what we have done:…").

In other words, "Business Continuity Management is the act of anticipating incidents which will affect critical functions and processes for the organisation {sic} and ensuring that it responds to any incident in a planned and rehearsed manner."[2]

Also, because most organizations have DR plans in place, they are likely to have identified their critical systems and assets…the ones they are most concerned to resume in the event of a disaster.

This paper, then, assumes that the process of critical asset identification is the same for DR planning and need not be reiterated simply for the purpose of the BC plans. In fact, it presumes that while the provision of critical assets must be resumed in the event of a disaster, with good planning most services need not be even significantly disrupted.

For those businesses who have not gone through the exercise of 'knowing thyself' there are numerous websites that contain good, if sometimes lengthy, models, papers, guides, and outlines for assessing risk and identifying critical assets.[3] All of these begin by emphasizing the absolute importance of undergoing a thorough business evaluation. This paper therefore does not attempt to recreate that crucial step.

After emphasis on the need to have critical assets identified, many BC models go to considerable pains to emphasize the importance of involving management (CEO level) support.

However, in the aftermath of September 11, 2001, it is spurious to think that management at the CEO level is not fully supportive of DR planning, and also if not convinced, then easily convincible, that BC planning is at the very least equally as important as that. (Or if they are not, I suggest that they never will be.) So this paper does not attempt to address that issue either.

The goal of this paper is simple. To present an outline of an actual BC plan that can be followed or improvised to fit differing organizations and business purposes. The BC plan from which the outline is drawn was created by this author in the two weeks between October 28, and November 9, 2001. It was subsequently reviewed and approved by internal auditors with minor revisions.

It is important to make the plan available to staff, to continue follow-up with them, and to make modifications often. This can only be done if it is truly considered a working document, no matter how complete it appears to be at any particular time. Staff change, options for resuming business change, the business itself changes. Keep the document updated. In fact, fit it into a routine process that is already in place, such as a change management process, or staff meeting schedule. It will not help if it is outdated in any way.

© SANS Institute 2000 - 2005 Author retains full rights.

Many aspects of the outline are intuitive, however, it is vitally important to have an understanding of the entire process before beginning. One must know the terrain one will be travelling through in order to be prepared for the trip. For that reason, it is strongly recommended that anyone who will use this outline first take advantage of the references listed, and it is suggested that any number of professional service vendors in the DR field can also be used as a information resources.

As a final note, the plan from which the outline is derived was developed for a state agency that serves as both the ISP, ASP, and PKI authority (as well as a user of its own services) for the majority of state governmental entities in the state. This includes Internet, mainframe, audio/video production, telecommunications, LAN and e-mail services, and the entire digital signature/authentication process. It is presented here in a scaled version, but may need to be either expanded or further scaled down to fit the needs of another organization.

It our situation, separate identically outlined plans were prepared for each building in which equipment and services are housed, and within each separate plan, each section was broken down into specific functional divisions. So, the original outline was filled in to create separate plans for each building, and within each building plan, the outline's sections were divided between the different functions housed in that building.

Annotations are in Italics.

© SANS Institute 2000 - 2005 Author retains full rights.

BUSINESS CONTINUITY PLAN

FOR

(company name)

© SANS Institute 2000 - 2005 Author retains full rights.

I. IMMEDIATE ACTION AND NOTIFICATIONS

NOTE:
This Section was created with the understanding that an emergency situation can occur at any time and first be observed by anyone in its proximity. The person who initially discovers the emergency situation may not know exactly what they are dealing with, or how to respond to it immediately. Once the situation is observed, and the 911 call has been made, the next actions can, and likely will, be made relatively simultaneously by management staff, and not linearly as a list suggests.

The following actions should be taken immediately upon awareness of crisis:

- **Call 911**
- Notify Critical Management Contacts (see list below).
- Notify Other Critical Organizational Contacts (see list below).
- Notify Guard Desk (see security guard information in Section VIII).
- Determine Course of Action to be Taken.
- Implement Evacuation Plan
- Provide Information/Instructions to Building Staff.
- Collect Administrative Operations Equipment as needed.
- Roll Out Action Plans by Service/Division/Function.
- Notify Critical Support Staff as needed (see list below).

Note:
The names and numbers below should include senior level supervisors at the corporate and executive level, as well as company personnel who will be responsible for decision making and be required to be involved in various aspects of the emergency. Following are suggested functionaries.

© SANS Institute 2000 - 2005 Author retains full rights.

CRITICAL EXECUTIVE CONTACTS	**OFFICE**	**PAGER**	**CELL**	**HOME**
Function Manager				
CEO				
Public Information Officer				
Security Manager				
Business Continuity Manager				
MANAGEMENT CONTACTS	**OFFICE**	**PAGER**	**CELL**	**HOME**
Other management whose function is affected either by proximity or a domino relationship				

© SANS Institute 2000 - 2005, Author re

© SANS Institute 2000 - 2005 Author retains full rights.

Note:
The following staff are intended to be those whose function within the organization may be critical for purposes of human resources, benefits, legal, property management, procurement or fiscal impact. This notification puts them on alert for possible questions or issues that arise as decisions are made.

CRITICAL CMS SUPPORT	**OFFICE**	**PAGER**	**CELL**	**HOME**

© SANS Institute 2000 - 2005, Author retains full rights.

II. EVACUATION PLAN

Note:
A pre-existing evacuation plan was modified to incorporate the possibility of long-term (at least one workday) evacuation. Additional "wardens" were assigned the responsibility of serving as an information coordinator. Those "wardens" will disseminate information about the nature of the crisis and what is expected of staff.

For our purposes, timekeepers were assigned the "warden" responsibilities.

Below is an example of an evacuation plan that allows the organization to accommodate both minor disruptions such as fire drills, as well as the more extended disruptions addressed in this paper.

Level I Emergencies:

In the event of a fire or a bomb threat, the fire alarm will signal to evacuate the building. In other Level I emergencies you will receive verbal instructions to evacuate the building from your Supervisor or Evacuation Warden. Please proceed as follows:

- Use the evacuation route given on the attached floor diagram.
- Stay away from windows whenever possible.
- Do not touch or disturb unrecognized objects.
- Leave the building by the exit closest to your descent route whenever possible.
- Find your Timekeeper and remain in his/her proximity until you receive further instructions.

Level II Emergencies:

An emergency will be designated Level II if the threat to employee safety is high, or if its nature is such that normal business in the building will be disrupted for 24 hours or longer. Examples of a Level II emergency are identification of an actual live bomb, or hazardous material. Your Supervisor or Evacuation Warden will inform you that a Level II emergency has been called. Please proceed as follows:

- Evacuate the building as in Level I emergencies.
- Proceed ON FOOT to the (name of a building or place that will suffice for staff to report to).
- Report to your Timekeepers and remain in his/her proximity until given further instructions.

© SANS Institute 2000 - 2005 Author retains full rights.

In Level II emergencies, certain employees are considered "critical" to continued business functioning. If you have been identified as a "critical" employee, report first to your Evacuation Warden, and then to your Supervisor for instructions.

III. CRITICAL STAFF AND CONTACT INFORMATION

Note:
Staff are considered critical if their duties and responsibilities are such that they must continue to function regardless of the nature of the emergency. There may be any number of 'divisions' within this outline, and any number of critical staff within divisions.

A: *Division Name*

Section Name:

Name, Section Manager
Office: ###-####
Home: ###-####
Cell/Pager: ###-####

Name, Function
Office: ###-####
Home: ###-####
Cell/Pager: ###-####

Name, Function
Office: ###-####
Home: ###-####
Cell/Pager: ###-####

Section Name:

Name, Section Manager
Office: ###-####
Home: ###-####
Cell/Pager: ###-####

Name, Function
Office: ###-####
Home: ###-####
Cell/Pager: ###-####

Name, Function
Office: ###-####
Home: ###-####
Cell/Pager: ###-####

B: *Division Name*

Section Name:

© SANS Institute 2000 - 2005, Author retains full rights.

Name, Section Manager
Office: ###-####
Home: ###-####
Cell/Pager: ###-####
Name, Function
Office: ###-####
Home: ###-####
Cell/Pager: ###-####
Name, Function
Office: ###-####
Home: ###-####
Cell/Pager: ###-####

Section Name:

Name, Section Manager
Office: ###-####
Home: ###-####
Cell/Pager: ###-####
Name, Function
Office: ###-####
Home: ###-####
Cell/Pager: ###-####
Name, Function
Office: ###-####
Home: ###-####
Cell/Pager: ###-####

IV. OPTIONS FOR ALTERNATE BUSINESS FUNCTIONING

Note:
In this Section, each division, or functional area, is responsible to identify how they will continue to function, where they will relocate, what equipment they will use/need, who will perform what tasks to mobilize continuity, etc.

In some cases voice communications or home bases were identified, in others alternate locations were found that could house surplus equipment or that had existing equipment that could be used on a temporary basis. In still other situations, an alternate was proposed that required new wiring, or was already part of the existing DR plan.

One plan was simply to set up card tables and laptops in an existing warehouse with phone lines.

© SANS Institute 2000 - 2005, Author retains full rights.

The administrative portion of this section concentrated on coordinating various interrelated functions, and keeping communication flowing between all parties.

The key to developing this section, and in fact to BC planning overall is flexibility and obtaining input from all parties to ensure all contingencies has been covered.

A:*Division Name*:

Section Name:
Brief description of alternative functioning option(s)

Section Name:
Brief description of alternative functioning option(s)

B:*Division Name*:

Section Name:
Brief description of alternative functioning option(s)

Section Name:
Brief description of alternative functioning option(s)

V. PLANS FOR SERVICES CONTINUITY

Note:
This Section involves providing a detailed description of how the division intends to function given the alternate location and functioning options provided in Section IV.
Once the relocation has occurred, managers are here required to explain how they will go about continuing their business.

A: *Division Name*:

Section Name:
Description of the way in which business functions will continue under the alternate location option identified in Section IV.

Section Name:
Description of the way in which business functions will continue under the alternate location option identified in Section IV.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

***B: Division Name*:**

Section Name:
Description of the way in which business functions will continue under the alternate location option identified in Section IV.

Section Name:
Description of the way in which business functions will continue under the alternate location option identified in Section IV.

VI. EMERGENCY CONTACT INFORMATION

Note:
Each employee should be required to provide names and contact numbers for the person(s) they want notified in the event of an emergency or other situation where notification is necessary. However, in the general distribution of the plan, this section is left blank due to privacy considerations. Supervisors and "wardens" were given this information only as it pertains to their staff. Upper management should have a complete copy, since the situation may require their intervention in an emergency.

The complete list is sorted alphabetically by person's name, and should be updated regularly.

Supervisor Name	Emergency Contact Name	Relationship	Contact Phone: Work	Contact Phone: Home

VII. SPECIAL NEEDS STAFF

Note:
Every employee was given the option to indicate that they have a special need. Needs that were identified included large screen monitors, wheel chair access, TDD service, and diabetes.

The chart includes a location column to easily determine where those staff offices are located. It should be reviewed frequently since staff changes will affect it.

Office Location	Division	Supervisor Name	Phone #	Home Phone	Cell Phone	Pager	Special Need

© SANS Institute 2000 - 2005 Author retains full rights.

VIII. SPECIAL SKILLS

Note:
Staff were asked if they had any special skills which may be useful in an emergency. Such skills as Emergency Medical Training, and CPR training were identified.

Division	Supervisor	Name	Phone #	Home Phone	Cell Phone	Pager	Skill

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

IX. GUARD CONTRACTS AND INFORMATION

Note:
Since most buildings that house information systems have some form of guard security, it is essential that they be kept informed of any situation as it develops. Guards will need instructions, and their supervisor/manager/vendor contact should be kept informed as well.

This Section should include details about the guard responsibilities/contract, shift information, guard names and phone contacts, and plans for how they are to proceed in the event of various emergency situations.

X. BUILDING BLUEPRINTS

Note:
In some situations it will be critical for emergency response personnel to have a building blueprint. It is strongly suggested that blueprints be available in electronic form as well as on paper.

XI. POTENTIAL CRISIS MITIGATION

Note:
All organizations have processes, physical layouts, procedures, or other things that can be identified as potentially risky. When given an opportunity, staff can frequently point out problems that when looked at could be changed to mitigate the danger. Once compiled, these problems should be reviewed and prioritized as to the action that can/should be taken.

The next step after they are identified is to follow-up and actually do the review.

A. *Division Name*:
Problem as identified.

B. *Division Name*:
Problem as identified.

XII. ITEMS REQUESTED TO BE OBTAINED

Note:
In every plan of this sort there will be some equipment, software, space, or other resource that should be obtained in order to ensure that the plan could work. As in Section XI, once identified, the items requested should be reviewed and go through the appropriate

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

procurement/approval process.

The list may include purchase of equipment, reallocation of equipment, assignment of rights to a system or application, or any other change in ownership or distribution that would allow the organization to continue business in an alternate situation.

A. *Division Name:*

Section Name:
Request and justification.
Section Name:
Request and justification.

B. *Division Name:*

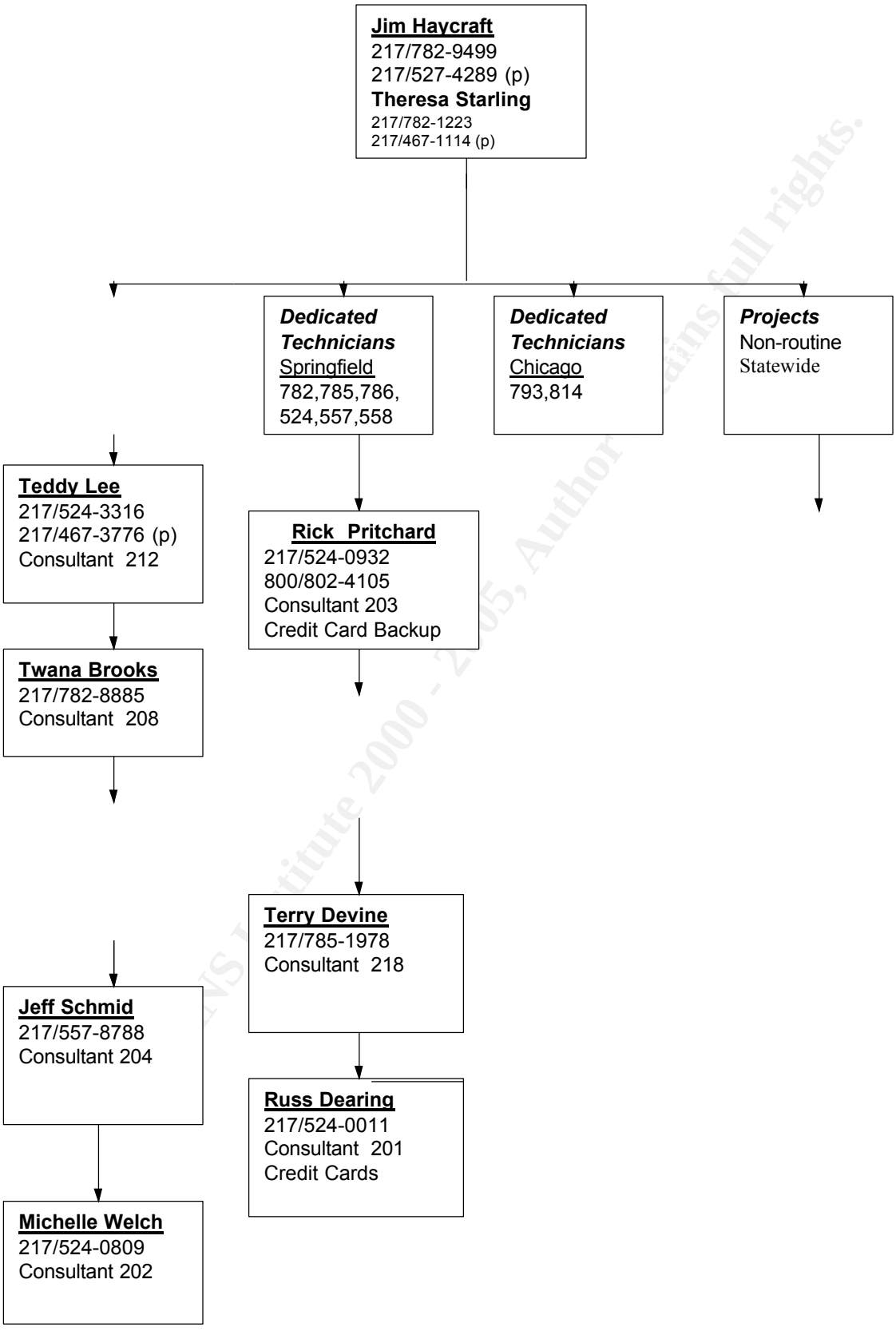
Section Name:
Request and justification.
Section Name:
Request and justification.

XII: Organization Charts

Note:

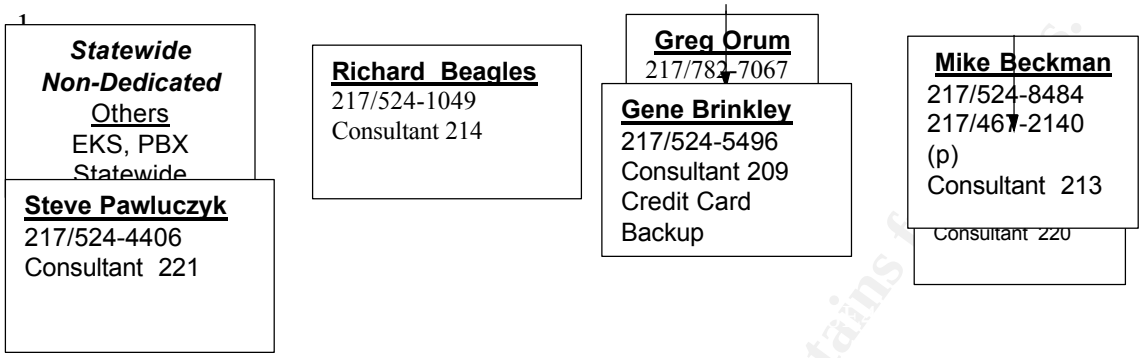
This section should include an organization chart for every division included in the plan. The charts will become useful in the event of a situation in which someone other than the normal supervisory staff is required to make decisions.

© SANS Institute 2000 - 2005, Author retains full rights.



© SANS Institute 2000 - 2005 Author retains full rights.

Footnotes



© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.