

Business Continuity Plan

Sicker Internet Webhosting Services

*Development of Plan:
Aaron Nielsen, Double A Consulting*

Version 1.1 (Updated: 11/12/2008)

Table of Contents

I.	Company History and Relevant Background Information	3
II.	Business Continuity Plan and Overview	4
III.	Project Management and Initiation	5
	a. Risk Analysis	5
	b. Management Support	5
	c. Establishment of Team	5
	d. Timeline	6
IV.	Business Impact Analysis	7
	a. Overview	7
	b. Gathering of Relevant Data	7
	c. Maximum Allowable Downtime	7
	d. Potential Business Losses Due To Outage	8
	e. Importance of Business Functions In Relation to Downtime	9
V.	Recovery Strategies	10
	a. Overview	10
	b. Emergency Team	10
	c. Primary Emergency Location	10
	d. Alternate Emergency Location	11
	e. Likely Scenario Plan	11
	f. Specific Scenarios	12
	g. Cost and Benefits	12
	h. Timeline for Return to Primary Location	12
	i. Recovery Steps Summary	13
VI.	Plan Design and Development	14
	a. Business and Service Recovery Plans	14
	b. Maintenance, Awareness, and Training	14
	c. Testing	14
VII.	Final Thoughts	15
VIII.	Update Log	16

I. Company History and Relevant Background Information

Sicker Internet Webhosting Services (SIWS) is a small internet hosting company founded by Douglas Sicker in 2000, based out of Boulder, Colorado. SIWS found a niche in the industry by providing webhosting for businesses in the Boulder-area, while providing in-town customer service for users in need of assistance. Douglas Sicker founded the company alone, though now nearly twenty employees are employed at SIWS. Additionally, though many of the customers are still located in the Boulder-Denver area, the company has grown to host websites for companies and individuals around the world. Hosting fees range from \$1.99/month and up. Currently, SIWS has 2,000 clients and advertises a 99% network uptime.

II. Business Continuity Plan Overview and Goals

This business continuity plan was developed by Aaron Nielsen of *Double A Consulting* and last updated in November 12, 2008. The only business continuity plan developed previously was inadequate and outdated for the current company size of operations. This business continuity plan will deal with contingency planning in the unlikely, but ever-present event of a disaster. In the event of such an incident, the following document will provide the details on how the event will be handled, who will be involved, and how the document will be updated in the future. Specifics of the contingency planning will include five phases:

- 1) Project management and initiation
- 2) Business impact analysis
- 3) Recovery strategies
- 4) Plan design and development
- 5) Testing, maintenance, awareness, and training

III. Project Management and Initiation

a. Risk Analysis

As a webhosting company, Sicker Internet Webhosting Services is providing nearly 2,000 customers with a service that necessitates that their network is up and running all the time. Unfortunately, though in an ideal world a network would have 100% uptime, this is not the case in a world where there are power failures, natural disasters, technology malfunctions, and human imperfections. Since customers are expecting their websites are up and running all the time (or very nearly), it is of the utmost importance to provide a plan in the case of issues stated above.

Sicker Internet Webhosting Services advertises 99% network uptime, in an attempt to compete with larger webhosting services like GoDaddy. Customers need a reason to not sign up with a larger company like GoDaddy and Sicker Internet Webhosting Services fills this void by providing not only superior customer service, but just as importantly, reliability. Not only is it important to hold to the promise of 99% network uptime for the sake of truthful advertising, but without this high level of network uptime, customers will likely not continue to use Sicker Internet Webhosting Services in the future and also, a negative, possibly irreparable damage to the image of the company. For these reasons, the viability of Sicker Internet Webhosting Services is reliant on its ability to be reliable.

b. Management Support

In cooperation with Sicker Internet Webhosting Services, C.E.O. Douglas Sicker approved this plan (see end of document for his endorsement). Upper management will be involved in taking steps towards enacting this policy by the beginning of next year (January 2009) and a short disaster preparation seminar is to be conducted for all technical members shortly thereafter. Accountability for the plan is extremely important and thus each item laid out in this plan will be individually assigned to upper management in the coming days. For future use, responsibilities placed in this plan will be reviewed on a yearly basis, so that all duties will always be the responsibility of some individual in the company.

c. Establishment of Team

C.E.O. Douglas Sicker (or any future C.E.O.) is responsible for approving the yearly updating and approval of this plan. Network security director (currently Jimmie Jones) is in charge of implementing this plan and for the updating of this plan. Further responsibilities in the plan will be delegated by the network security director.

d. Timeline

This plan has submitted to Sicker Internet Webhosting Services CEO Douglas Sicker for immediate approval. By year's end (and each subsequent year's end), this plan is to be implemented and re-approved by the company CEO. Additionally, this January (and each subsequent January), a short one-hour disaster preparation seminar will take place with all technical members of the staff.

IV. Business Impact Analysis

a. Overview

This section on Business Impact Analysis will examine how a disaster will affect Sicker Internet Webhosting Services, whether it has to do with the company's productivity, finances, reputation, or ability to respect regulations. Included in this analysis, gathering of data involving business impact will be discussed, the maximum allowable downtime will be considered, potential losses will be outlined, and how business functions will be prioritized in the event of a disaster will be studied.

b. Gathering of Relevant Data

With Sicker Internet Webhosting Services being in the webhosting industry for nearly ten years, a few long-time customers exist and they will be very important in helping assess how the company could be impacted if downtime occurs.

Network security director will approach approximately twenty of these long-time customers and will offer a discount on the customer's bill in exchange for their cooperation in a short ten minute telephone questionnaire. The contents of this interview will involve how the customer would potentially deal with network downtime, their tolerance of network downtime, and how they would like to be contacted in the event of an extended downtime.

Results of this data collection will be used in conjunction with this document for a yearly re-evaluation and re-approval of this plan. Should the customers suggest that a higher reliability be required than is currently advertised, this plan will have to be re-assessed.

c. Maximum Allowable Downtime

Currently, Sicker Internet Webhosting Services advertises 99% network uptime. In terms of minutes per month, this rate of network uptime would require all but seven hours a month that the webhosting services be operating. Now it should be noted that though it is essential that the webhosting services down less than seven hours a month, other services could possibly be down for more than seven hours a month and still be acceptable. This will be examined in the coming sections. With seven hours per month as the maximum allowable downtime for the company's webhosting services, several considerations will be need to be considered, including how the company can withstand even a minor disaster without the company's webhosting services to even be down a single night per month.

d. Potential Business Losses Due To Outages

Chief among the business losses due to outages would be those concerned with the company's reputation and ability to keep customers using Sicker Internet Webhosting Services in the future. The company's reputation is essentially staked on keeping 99% uptime, so any violation of this agreement could result first in the loss of current customers and also result in the loss of future customers.

Should the webhosting services be down more than two consecutive hours, customers that are using the service for commercial purposes will be taking possibly significant losses. Due to this consideration, potentially the first customers that could quit using Sicker Internet Webhosting Services in retaliation of an extended downtime would be online retailers and this possibility is devastating. Having a clientele of online retailers provides a great image for Sicker Internet Webhosting Services. Additionally, since online retailers usually require greater bandwidth and storage requirements, they are paying higher monthly fees than a typical individual, who is currently using the company's services just for a personal website. Approximately 30% of the company's income is currently from online retailers. It is estimated that up to 50% of these customers (or 15% of the total income of Sicker Internet Webhosting Services) could be lost due to one extended downtime. These reasons only reinforce the necessity of minimizing webhosting downtime.

The company's reputation is also at stake when considering excessive downtime. As the company developed in the previous years with numerous customers in the Boulder-Denver area, a number of new customers have come from current customer's recommendations. The company prides itself on a good image in the customer's eyes, so word of mouth will help the company grow. Potentially, 10% of new customers could be lost if this word of mouth is negative about the company.

Not only would a webhosting services downtime of more than seven hours per month result in customer disapproval and possible financial losses, advertising regulations should also be considered. The backbone of the company is advertised the 99% uptime. If the company fails to uphold this claim, it could no longer be used in advertisements and could result in the loss of new customers. To compete with bigger companies such as GoDaddy, it is important to offer an equivalent alternative and if Sicker Internet Webhosting Services cannot provide 99% uptime, customers will choose the alternative company. Without having the 99% uptime in advertisements is essential to compete in a crowded market. It is estimated that 50% of new customers could be lost if the company cannot advertise a 99% uptime.

e. Importance of Business Functions In Relation to Downtime

It is very important to consider how Sicker Internet Webhosting Services will prioritize in the event that the company is impacted by a disaster. As outlined in the previous sections, the highest priority is the webhosting services. These services can be down on average seven hours a month without serious repercussions. This small time window means that in the event of a disaster, the company must be motivated in quickly re-establishing the webhosting services fastest. Though the steps to be taken to re-establish these services will be examined in the following section, it should be noted for its priority.

In cooperation of the re-establishment of webhosting services, a customer service phone line should be re-established. If this is not possible due to building damage or other reasons, the company should work with the phone company to have all phone calls forwarded to the alternate location (to be discussed later).

After establishing/re-establishing webhosting services and a customer service phone line, data backup is next in importance. With the web services running, it is important to maintain the integrity of the customer's files. Though it is possible to run the web services without data backup for a short period of time, it is not practical to consider this a long-term possibility.

Next in priority of business functions is the internal company servers and technical staff member's ability to use the network. The company could potentially have a downtime of several consecutive hours for technical staff members without a huge loss, but it should not exceed more than one consecutive day twice a year. Productivity of the company will decrease should technical staff members not be able to work more than two days a year due to network problems. The final priority is the re-establishment of administrative network abilities. In the unlikely event of a disaster, the administrative network abilities are the least important and any of their potential duties will have to be performed on pen and paper (ie, note taking, calendar scheduling, etc).

Below is a summary of the priorities beginning with the most important:

- 1) Re-establishment of webhosting services at primary location if possible
- 2) Transportation of webhosting services' hardware to alternate location if necessary
- 3) Reconnection of customer service phone line
- 4) Call-forwarding to alternate location if primary location is compromised
- 5) Re-establishment of technical employees' network access
- 6) Re-establishment of administrative employees' network access

V. Recovery Strategies

a. Overview

This section on recovery strategies will focus on how Sicker Internet Webhosting Services will specifically deal with a potential disaster. Specifically, an emergency team will be outlined, the possible locations in case of an emergency will be discussed, a plan of a likely scenario will be laid out, specific scenarios will be considered, overall cost and benefits of recovery strategies will be outlined, and finally, a summer of recovery steps will be presented.

b. Emergency Team

The emergency team is presented below, followed by a signoff by Sicker Internet Webhosting Services CEO affirming the current job duties. In case of an emergency, the following team has been outlined. The primary and secondary contacts below should be contacted first if the event of an emergency

Emergency Team Manager/Network Security Director/Primary Contact:

Jimmie Jones (303) 484-1673

Emergency Team Assistant Manager/Secondary Contact:

Barbara Kay (970) 223-2121

On Call Security Company:

Totally Safe Security (303) 765-7600

Emergency Customer Service Representative

Jenny Lewis (303) 980-2345

Company C.E.O.

Doug Sicker (303) 495-1678

Approved by: _____

Date: _____

c. Primary Emergency Location

In the event that a disaster has not rendered the primary location unusable, the following, current location will be used.

Sicker Internet Webhosting Services

1621 Pearl St.

Suite 130

Boulder, CO 80303

d. Alternate Emergency Location

In the event of a disaster that has rendered the current location unusable, the temporary, alternate location is the personal residence of Doug Sicker. Specifically, the network can be set up in company C.E.O. Doug Sicker's unfinished basement. This alternate location can be used for up to a week, yet due to the bandwidth limitations of Doug Sicker's internet connection, this alternate location should only be considered for up to two days. In the event that a disaster has rendered the primary location unusable for more than two days, Instant Access Service Bureau should be contacted at (303) 234-1234 immediately for their short to medium term services.

Doug Sicker Personal Residence
4011 Arapahoe St.
Boulder, CO 80309

e. Likely Scenario Plan

In this section, a likely scenario will be considered. Since the company requires twenty servers, a high bandwidth internet connection, phone service, and approximately 1,000 square feet of workspace, backup hardware is important. Consisting mostly of older hardware, there are currently ten servers stored in Doug Sicker's basement and can be used to re-establish webhosting services in the event that servers at the primary location are compromised. Additionally, a previously used multiple line, multiple handset phone is available for use at the secondary location. Currently, all data is backed up daily on a tape drive at the primary location and at Doug Sicker's personal residence. Should the primary location's tape drive be compromised, the alternate tape backup can and should be used.

In the most likely scenario, a fire or a hardware failure could cause the webhosting services or the internal network to fail. Depending on the failure, the previous section (V) should be reviewed on prioritizing how to re-establish services. First, the emergency team should be contacted and should convene immediately either at the primary location or the alternate location. This document should be reviewed immediately and steps should be taken to counter the issue. A failure of one of the servers can be easily countered by using one of the alternate servers. If a piece of hardware fails that does not have a replacement on hand, two options should be considered. Replacement of the hardware can be completed, though this may take one or more days. Online or in-town retailers should be considered. Additionally, there is currently a cooperation agreement with James' Network Services located in Boulder, CO for emergency hardware needs. Part of the agreement requires we provide James' Networking Services with hardware in the case of their need.

f. Specific Scenarios

To prevent in the case of a flood, the servers are currently located one foot off of the floor. Additionally, the office is currently on the third floor, which should help prevent such a situation. If a flood does render some of the hardware unusable, usable hardware, emergency short-term hardware from James' Network Services, and new purchased hardware should re-establish the network at the primary location. If the primary location is not available, then the hardware should be relocated to the alternate location.

In the case of a structural failure or another disaster where the company's hardware is completely rendered unusable, all customers should be contacted immediately to be informed that the network will be down indefinitely and they will be credited accordingly on their bill. The emergency customer service representative will be making the contact with customers.

g. Costs and Benefits

Due to the small size of Sicker Internet Webhosting Services, a large amount of money cannot be invested in protecting against an emergency. Spending too much money on an unlikely situation for a small company is simply not a good investment. Current preparations allow for a free, temporary, alternate location at Doug Sicker's place of residence. Older hardware has been stored at his residence in the case that some or all of the network hardware fails. Additionally, a "no-cost" cooperation has been struck with James' Networking Services to help provide some security in the case of an emergency. It should be noted that this cooperation will not provide the necessary hardware in the necessary timeframe. In that case, an in-town purchase of new hardware should be completed immediately and future insurance reimbursements will pay for these costs. The company currently has \$100,000 credit line to spend on hardware in the case of an emergency. Though a hot-site and/or a complete backup set of hardware is optimal, it is not financially feasible in this situation.

h. Timeline for Return to Primary Location

The goal is to return all operations to the primary location within two business days if the alternate location is used. If this is not possible, a medium-term option has been laid out previously and should be considered in the event that the primary location is unavailable indefinitely

i. Recovery Steps Summary

- 1) Contact Emergency Team
- 2) Convene at Primary Location
- 3) Convene at Secondary Location if necessary
- 4) Lay out necessary steps to re-establish webhosting services
- 5) Re-establish webhosting services, even if at non-optimal performance
- 6) Transport hardware to alternate location if necessary
- 7) Contact James' Networking Services if hardware is needed for webhosting
- 8) Contact Instant Access Service Bureau if in need of medium-term assistance
- 9) Purchase new hardware for webhosting if necessary
- 10) Establish a customer service phone line if current line is down
- 11) Forward calls to alternate location if primary phone line is unusable
- 12) Re-establish internal network services for technical staff members
- 13) Re-establish internal network service for administrative staff members

Approved by: _____

Date: _____

VI. Plan Design and Development

a. Business and Service Recovery Plans

Please refer to section V(h).

b. Maintenance, Awareness, and Training

This plan should be reviewed annually, necessary changes should be enacted to this document, and re-approval by company CEO should be completed.

Additionally, every January, a one-hour seminar should be conducted with all emergency response team members to keep them up to speed on current emergency procedures. In the event that an employee currently on the emergency team resigns from the company, a replacement should be found immediately and approved accordingly.

c. Testing

In conjunction with the annual seminar, a “mock-disaster” scenario should be given to the emergency team members. Their “mock-response” should be noted and assessments by the network security director should help improve their response.

VII. Final Thoughts

This document has laid out the plan for Sicker Internet Webhosting Services in the case of a disaster. Considerations have been made for multiple scenarios and prioritizing how services should be re-established has been outlined. In the event that the necessary information cannot be found in this document, the network security director should be advised.

Please note that this document should be placed online on the company's website, a hard copy-copy should be on-hand at the primary location, a hard-copy should be placed off-site with the company CEO, and a hard-copy should be placed off-site with the emergency manager.

Final plan approved by: _____

Date: _____

VIII. Update Log

Version 1.1: November 12, 2008

Version 1.0: November 8, 2008