

RE: Disaster Recovery Plan

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2004-06/0257.html>

From: Holmes, Brian (*Brian.Holmes_at_corelab.com*)

Date: 06/23/04

Date: Wed, 23 Jun 2004 14:47:41 -0500

To: "ka55ad" <ka55ad@gmail.com>

What you described sounds more like a "backup strategy" which is incorporated into a DRP. The DRP itself should be based on priority and risk levels.

1st step:

Assess the computing environment and determine the acceptable risks and/or downtime (e.g. how long the environment(s) could remain down w/o significantly affecting the business?)

2nd step:

Document all the information required to "rebuild" the systems: hardware, software, applications, system configuration, licenses, etc...

3rd step:

Prioritize the system restoration process, i.e. what systems should be up first, etc... Since some systems are required to operate other systems, consider this (e.g. must restore OS before loading Apps)

Note: Make sure to include the process for restoring the data – the person who normally does this may not be available in a disaster, so write clear and concise instructions.

4th step:

Test the plan...

Attempt to justify the costs of implementing and testing a solid DRP by quantifying financial loss to management. For example, if the data center was flooded, the company would lose all computing for 4 days. Due to the nature of our business, this could cost us over \$1,000,000. Therefore, it is in our best interests to invest in a solid DRP.

Brian Holmes

IT Business Analyst

Core Laboratories

phone: (713) 328-2679

fax: (713) 328-2901

bholmes@corelab.com

SecurityFocus BASICS: RE: Disaster Recovery Plan

-----Original Message-----

From: ka55ad [mailto:ka55ad@gmail.com]
Sent: Tuesday, June 22, 2004 8:53 AM
To: security-basics@securityfocus.com
Subject: Disaster Recovery Plan

Although this might be slightly off topic, I was wondering if anyone could give me some suggestions for some disaster recovery plans. Right now we are a small place (less than 50 employees total), and I am not comfortable with the current Disaster Recovery plan (it was created before I came on board). It basically involves performing a master backup on tape once a month and then doing a differential backup every week night. We have 2 sets of differential tapes that we keep off site and alternate every week, but the masters are not kept off site.

I am working with a very limited budget. Can anyone recommend a good solution that will ease my worries? Thanks.

Ethical Hacking at the InfoSec Institute. Mention this ad and get \$545 off any course! All of our class sizes are guaranteed to be 10 students or less to facilitate one-on-one interaction with one of our expert instructors. Attend a course taught by an expert instructor with years of in-the-field pen testing experience in our state of the art hacking lab. Master the skills of an Ethical Hacker to better assess the security of your organization. Visit us at:
http://www.infosecinstitute.com/courses/ethical_hacking_training.html

Ethical Hacking at the InfoSec Institute. Mention this ad and get \$545 off any course! All of our class sizes are guaranteed to be 10 students or less to facilitate one-on-one interaction with one of our expert instructors. Attend a course taught by an expert instructor with years of in-the-field pen testing experience in our state of the art hacking lab. Master the skills of an Ethical Hacker to better assess the security of your organization. Visit us at:
http://www.infosecinstitute.com/courses/ethical_hacking_training.html