the Availability Digest

www.availabilitydigest.com

A Personal Failover Fault

Dr. Bill Highleyman
March 2013

Availability is all about providing a service, no matter what. The “no matter what” struck me during a presentation at the Connect OpenVMS Boot Camp, held recently in Bedford, Massachusetts. As editor of the *Availability Digest*, I was to give a talk entitled “Help! My Data Center Is Down!” It describes incidents taken from the Digest’s Never Again series of horror stories, incidents that have incapacitated entire data centers for hours and even days.

As I was booting up the PC on which my slides were stored, I experienced my own horror story. My PC was taken over by a malicious virus (or so it seemed to me) and became unusable. I was about to become one of the incidents of which I was to speak.

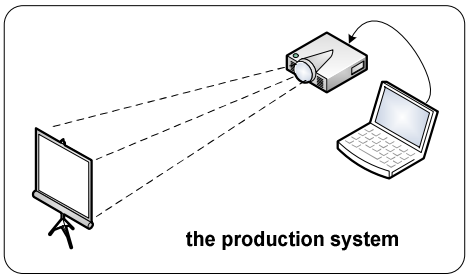
My talk ends with lessons learned to keep the business going in the face of such incidents:

1. Employ redundancy to protect critical systems from failure by failing over to backup systems.
2. Have a failover plan.
3. Practice the failover plan to ensure that it works and that staff is trained.
4. If all else fails, be sure to have a business-continuity plan that maps out how you will maintain services in the absence of IT support.
5. Communicate with your stakeholders to keep them informed about the problem and your progress in restoring service.
6. After recovery, perform a root-cause analysis; and institute procedures to prevent the problem in the future.

Did I follow my own advice? Let’s see.

The Production Service

The service that I was to provide was to give my presentation to a room full of people. To that end, I had prepared my slide set and had it stored on my PC. I had practiced the talk to ensure that its length was compatible with the one-hour time slot. In fact, I had previously given the talk successfully several times, including several Availability Seminars as well as at HP Discover 2012 and the 2012 NonStop Technical Boot Camp.



The previous speaker finished on time, and I went to the front of the room to set up. I plugged in the power cord and connected my PC to the projector. I turned on the PC; and while it was booting, I fiddled with the lapel mike to make sure it was working.

With the room now full of attendees, I turned my attention to the PC to bring up PowerPoint, select my slide set, and begin the presentation. The display sprang to life and projected itself on the eight-foot screen. And there, to my horror, I saw the intruder.

The Outage

Well, maybe it wasn't a malicious virus. But it might just as well have been. Displayed on the screen, was the message "*Configuring Windows updates. 5% complete. Do not turn off your computer.*" My PC had been wrested from my control and was useless. So far as the presentation was concerned, my PC was down.

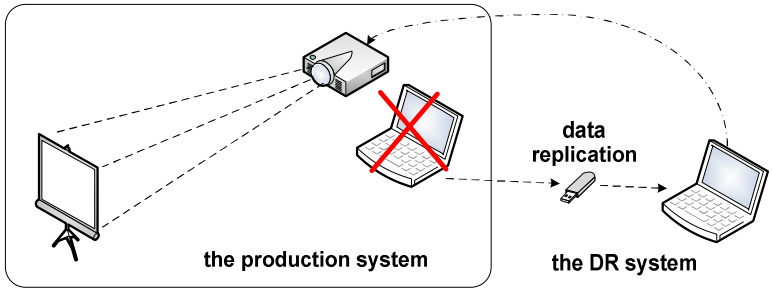
For some reason, Windows did not give me a warning that it was about to do this. Usually, it asks permission and lets me delay the upgrade if I want. Perhaps it had given the warning before I shut down the PC previously, and I hadn't seen it. In any event, panic set in.

Hoping that I could stop Windows in its tracks, I rebooted the PC. After a couple of minutes, it came back on; and Windows continued with its nefarious deed. Powering off didn't work. Even worse, the upgrade was proceeding painfully slowly. As the entire room tried to contribute a solution, the upgrade hadn't progressed beyond 5%.

The Disaster-Recovery System

Fortunately, I had prepared for such a disaster. I remember too many times in the early days of PCs when I couldn't get my PC to cooperate, and I had made it a practice to bring transparencies to use with an overhead projector if need be. Overhead projectors and transparencies are now a thing of the distant pass, but failures are not.

My backup strategy is now to replicate my slides to a memory stick so that I can use another PC if mine should become inoperable. In fact, to be super safe, I always bring two backup memory sticks with me.



So now all I had to do was to deploy another PC.

The Failover Fault

How do I acquire another PC? My plan had always been to ask the audience if I could borrow someone's PC. I am sure that I would have multiple offers.

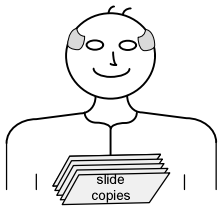
Unfortunately, I had never tested this failover plan; and it ran into a fairly simple problem. I forgot that this was my plan. When things go wrong, people (including me) get stupider. In hindsight, I wonder if I would have been too embarrassed to ask for someone's computer even if I had remembered. I don't know. Again, I had never tested the plan.

I froze and watched the screen – "*Do not turn off your computer. Windows is 10% completed reconfiguring.*"

The Business Recovery Plan

Now I was really down. I had lost my production system, and I had been unable to execute a successful failover to my disaster-recovery system. Fortunately, I had a Business Recovery Plan (BCP) that would allow me to continue to provide the presentation even in the event of a dual failure.

The Business Recovery Plan was straightforward. I had printed out a copy of my slides and had them with me. I was able to begin the presentation by referring to my printed copies. After about twenty minutes, Windows finally completed its update and returned my computer to me. I brought up PowerPoint and completed the presentation with the displayed slides. My total downtime was about five minutes, and I was able to finish on time.



business continuity plan

In hindsight, a more effective BCP would have been to bring multiple copies of the slides with me and pass them out to the audience. Then we all could have had the benefit of the slide set. However, this is a cost and convenience factor. For the unlikely probability of having to pass out copies of the slides, is it worthwhile printing and bringing in a large stack of paper? This is not a very green solution. Besides, how many copies should I print? I have decided not to extend my BCP to this technique.

Stakeholder Communications

In this incident, the stakeholders were those sitting in my audience. Communication was inherent in the process. Everyone knew what happened, everyone knew what was being done to try to recover, and everyone was very supportive – even jovial.

The Root Cause

After a failure incident, it is important to perform a root-cause analysis to determine what caused the outage and what can be done in the future to prevent it. The cause was obvious, but I had no idea as to how to avoid it in the future. If Microsoft is going to commandeer my computer without my permission, what am I to do?

One thought was to kill the Internet connection. This will work if the hijacker is in the process of downloading the updates. But if the updates already have been downloaded, I suspect that the Internet is not involved in the configuration of the updates.

My coworker solved the problem. Searching around, she discovered the program named, amazingly, “Windows Update.” Windows Update can be accessed from the Control Panel. One of its options is “Change settings.” A drop-down list provides four choices:

- Install updates automatically (recommended).
- Download updates but let me choose whether to install them.
- Check for updates but let me decide whether to download them or install them.
- Never check for updates (not recommended).

I am now running under option 3. I let Windows ask me if I want to download and install updates, which I will always do when convenient. Now I have control of my PC.

Summary

I write and lecture a great deal on high availability. It is refreshing to see that the principles of achieving high availability apply even to simple systems and that I got at least a passing grade in applying them. I wasn't perfect, but the service survived at an acceptable level.