the Availability Digest

www.availabilitydigest.com
@availabilitydig

# The High Availability Design Spectrum – Part 4

Dr. Terry Critchley

March 2017

[Editor's Note: In his book "High Availability IT Services," Dr. Terry Critchley lists twenty-three areas that can have an impact on the availability of IT business services. In this multipart series, and with his permission, we publish his observations. In Part 1 of this series, we reviewed his first four reflections - his Parts A through D. In Part 2, we examined his next nine considerations – his parts E through M. Then in Part 3, we published his six observations N through S. In this final Part 4, we publish his last four opinions, T through W.]

Dr. Terry Critchley: Most of the documentation on HA/DR I have come across majors on hardware, mainly redundant or fault-tolerant, and to some extent software. My thesis is that the spectrum of activity needed to design, implement and maintain a high availability business IT system and recover from failures small and large (DR) is much, much greater. Below, I have listed 23 areas (A to W) that can have an impact on the availability of business services that are IT-based. I am sure it will be evident that these areas can have a significant impact on the availability and non-availability of any service or system.

Remember, focusing on availability and focusing on avoidance of non-availability are not the same thing if you think about it.

The book and chapter references following refer to 'High Availability IT Services':
https://www.crcpress.com/High-Availability-IT-Services/Critchley/9781482255904.

## T. Availability by Teamwork

Marty Brounstein, in *'Managing Teams for Dummies,'* lists ten qualities necessary for effective teamwork. The headings of team member qualities are reproduced here.

1. Demonstrating [*personal*] reliability
2. Communicating constructively *[this includes documentation in my opinion*]
3. Listening actively [*remembering he/she has two ears and only one mouth*]
4. Functioning as an active participant [*no passengers or deadweights*]
5. Sharing openly and willingly (information, knowledge, experience *[no bragging though*])
6. Cooperating and pitching in to help [*nothing to contribute here - fetch the coffee*]
7. Exhibiting flexibility [*change is inevitable - swim with it, not against*]
8. Showing team commitment [*no 'sickies' to watch a ball game*]
9. Working as a problem solver [*especially useful in Delphi exercises*]
10. Treating others in a respectful and supportive manner [*giving 'strokes']*

In my usual style, I would add another quality to an excellent list - *good timekeeping,* and a quotation to support item 3 above:

> "I like to listen. I have learned a great deal from listening carefully. Most people never listen." - Ernest Hemingway

However you define 'good' teamwork, a good team will design, implement, operate and maintain a better HA/DR system than a 'so so' or downright 'poor' team. Also, a team is probably only as good as its worst player.

## U. Availability by Organization

High Availability and Disaster recovery (HA/DR) are (or should be) becoming more important in business IT, which means that IT is evolving. It stands to reason that if business IT and its requirements are evolving, then the organization of people using and supporting business IT should evolve in line with the much-vaunted principle of 'aligning IT with the business'. What does this mean in practical terms?

- appropriate parts of the business community should be HA-aware, meaning they understand the principles of HA/DR, what it means to the company's business and what their role in it is. Each business 'unit', however that is defined, should have an HA/DR-aware person, not necessarily full-time, plus a deputy or substitute
- IT skills should be regularly reviewed in the light of the evolution of IT requirements and the evolving nature of any threats to the stability of that IT, be it malware, performance, functionality or anything else that might breach SLA requirements and specifications.

## V. Availability by Eternal Vigilance

This is a key factor in keeping the show 'on the road' and relates to the ***security aspects of systems and services***. A compromised system may be 100% available but unable to perform its allotted functions because of lost functionality or data caused by a *malware* attack. This item never appears on outage surveys over about 10 to 15 years old as the problem was virtually unknown, particularly in large organizations.

Today, it is not unknown. It may now be known but it is not fully understood. Moreover, even where it is understood, there is often little proactive activity in the monitoring, detection and mitigation of such attacks. Such activity is encompassed in SIEM (Security Information and Event Management - Gartner 2005), outlined in Chapter 7 and other papers referred to in this book.

Analysis of **security event logs** helps security analysts detect and investigate advanced threats often missed by simple tools or manual methods. Good security analysis provides converged network security monitoring and centralized security information and event management. Threats are not necessarily what the EMC reference below calls *'smash and grab'* but often involve illicit seeding of malware entities on a system to facilitate malicious and potentially damaging access to systems and data.

There is also a **liveware aspect** to this area since software tools cannot really monitor people and they are often potential 'criminals'. Methods and processes need to be adopted and revised so that the opportunity for system damage by people - both internal and external - is reduced to a minimum. Even then, that minimum should be worked on in the light of experience in one's own organization and in others, although companies are often loath to admit that their defenses have been breached.

**Physical security** beyond simple lock and key mechanisms are in use or available today to counter some liveware threats, among them:

- RFID badges for unattended access
- Security personnel and normal identity badges
- Face and iris recognition techniques

- Video/CCTV surveillance at entry points and around location/campus perimeters
- Fingerprint scanning
- Body heat detectors

Often, data theft is not just a case of stealing data by network or other non-physical intrusion but by walking away with smaller systems completely, as happened more than once at one of the companies I worked for in the past. It was rumored that these systems were 'stolen to order' as the stolen items were not just random pieces of IT equipment but complete systems. A solution here might be position sensing devices used to track stolen cars ('trackers').

### W. Availability by Location

It goes without saying that the location of data centers - primary and disaster - needs careful consideration, especially in areas prone to extreme weather conditions, earthquakes, 'sink holes' or other disruptive influences. For example, it is not recommended that you place your data center in the middle of the Bristol Channel as a location 'finder' did in England based on information fed into a program.

You also need to consider the supply and possible re-supply in emergency of:

- people
- power, water (controlled), other 'eco' supplies
- accommodation
- documentation (copies of *current* documents)
- communications - electronic and transport
- medical support
- other things connected with your IT and business and essential to its continued operation day to day.

There are a number of articles on the web dealing with location selection, but don't forget to think about your own particular business and needs. No 'blind following' of checklists.

***Final Words***: If you understand these areas of availability, do something about them. If you don't, take advice and then do something about them. Don't pay a third party lots of money for a report that sits on a shelf gathering dust. See the references listed below.

http://uk.emc.com/collateral/software/solution-overview/h11031-transforming-traditional-security-strategies-so.pdf

http://reports.informationweek.com/abstract/21/11076/Security/How-Attackers-Target-and-Exploit-Critical-Business-Applications.html?cid=SBX_iwk_fture_Analytics_default_newsletters&itc=SBX_iwk_fture_Analytics_default_newsletters