

## Business Continuity and Disaster Recovery and Healthcare.

### “CONSIDERATIONS

for Healthcare Organizations.”

#### Background

Mandated by the Health Insurance Portability and Accountability Act (HIPAA,) Healthcare providers must have a Disaster Recovery Plan, data backup plan, emergency mode operation plan and a risk assessment.

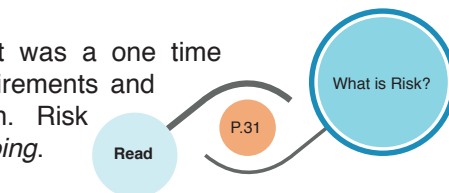
Many facilities performed the risk assessment requirement after the first big push in 2005 and then filed it away some place collecting dust. Security experts agree, that is a big mistake.

Healthcare CIOs and their IT steering committees have a lot on their plate these days with emerging technologies demanding attention and the average budget being 1-3% of operating revenue. Attention is greatly focused around barcode medication administration, physician documentation and interactive patient portals.

Demands on the Healthcare CIO are tight. The world of emergency response, business continuity, disaster recovery and general “end of the world as we know it” products and services is full of facts, fictions, and flux; and the noise on this channel is louder than ever as vendors jockey for position and highlight surveys and analyst quotes to justify their position and gain market share.

Some may think a risk assessment was a one time thing that we do for regulatory requirements and file away, but we need to think again. Risk Assessments are suppose to be *ongoing*.

A Risk Assessment is the first step in an ongoing Business Continuity and Disaster Recovery life cycle.



#### NEW ORLEANS August 23, 2005 – Katrina

After dealing with the surge of sick and elderly seeking shelter from a killer hurricane and a total loss of operational control, Charity and University Hospitals might have thought they had survived a catastrophic event that even the best contingency plans could barely handle. However, the worst was yet to come.

Days after the storm subsided, on the 8th of September, 2005, Richard Angelico of WDSU Channel Six in New Orleans reported: *“The health care system is dealing with another major ordeal -- its computers. The hospital’s IT system was in New Orleans and they lost it. For some reason, their backup system also failed. Now, they have Internet access only on five laptops in their “war room”.”*

#### OUR TOWN Today – The Board Room

We, and many others may be tasked with planning for an event like Katrina, or other types of disasters. Board Members are using words like “Disaster Recovery Plans,” “Business Continuity” or even “Continuity of Operations,” and they are looking to us for answers. Where do we start? What are leading practices? How do we alleviate concerns and maintain “business as usual” so our customers can focus on their core competencies?

#### Know the Terrain

“Disaster Recovery,” “Business Continuity” and “Continuity of Operations” are not the same things. These terms are often confused as a result of years of buzzword status and few standards. Here’s what we should know.

**Disaster Recovery** is the practice of designing a repeatable, living process in data center operations environment that allows a customer to rebuild critical systems at a secondary site after a catastrophe. It is not Operational Resilience (servers that fail over to one another in the same building). It is *not* Business Continuity.

**Business Continuity** can best be described as the manual workarounds and other ad-hoc solutions that nurses, doctors and other health care staff would use during an interruption to critical data center systems that support their jobs functions. Business Continuity is about doing what a hospital does without support systems and applications running.

Finally, **Continuity of Operations** is a catchall term used by Federal agencies and the military to sum up all of these efforts. Warning: do not let tricky vernacular leave you holding the responsibility for recovering systems and business processes after a disaster. Stay focused on Disaster Recovery, and use other Contingency Planning and Business Continuity initiatives as levers for your activities.

### **Understand the Drivers**

Understanding the drivers is an important aspect of the Disaster Recovery process. HIPAA regulatory issues, increased concern about pandemic flu and other bioagents, computer fraud and malicious hacker attacks, the terror threat and market volatility are all drivers for Disaster Recovery. Think past 911 and Katrina to the risk of tomorrow to better understand the risk of today.

### **Develop a Repeatable Process**

Disaster Recovery is a process, not a project. As your environment changes, so will your disaster recovery plan. While there are many vendors who would like you to believe that there is a so-called “killer app” they have that will make your woes go away, the reality is that a sound, repeatable and sustainable Disaster Recovery plan requires a program focus.

Using a continuous improvement approach to Disaster Recovery will refresh your outlook to risk, impact, backup and recovery, planning and testing year after year.

### **Know What’s at Risk**

A common mistake made by many health care CIOs is to assume what’s important to the organization and then throw the latest (and most expensive) technology at the problem. Stop. Think. Listen.

In the daily operations of a health care data center, what’s “important” from an IT perspective is based on gut at best, and in the worst-case scenarios, based on the “squeaky wheel” phenomena. That is, the application that breaks most often or is complained-about by the staff most often is the thing that is most important.

Without involving the right stakeholders in Business Impact and Application Impact Analyses, IT will always be off, in terms of ranking application criticality for Disaster Recovery.

### **Involve the Right Stakeholders**

Hospitals operate on different principles from those of manufacturing companies or other private industries. Understanding these differences is important when engaging third party consultancies for Business Impact

Analysis work that supports Business Continuity, and the related Application Impact Analysis that directly impacts how and when systems are recovered.

Involving the right stakeholders with the right perspectives is critical to the success of prioritizing systems for Disaster Recovery. While financial impacts are helpful in prioritizing systems for administrative and billing functions, these alone are not categorized in “sales” terms, as they would be for other industries. Health care concerns are driven by financial impacts such as longer stays, scheduling changes, malpractice suits and cross-departmental inefficiencies, especially in today’s world of digital radiology and other filmless image storage and retrieval.

Other key impacts are clinical in nature and include real-time monitoring, tracking and placement of patients, road-mapping and treatment timing, and patient flow as supported by systems such as PACS, McKesson and other clinical data systems.

Involving business, clinical and community support interests in your ranking of application criticality is a leading practice for CIOs in the health care industry, and partnering with third party vendors who understand medical-care needs is paramount.

### **Choose A Second Site Wisely**

While many hospitals are using “hot sites” or choosing on-campus second data centers, choosing a second site wisely is the key to recovering systems and servicing patients. The second site must be near enough to the primary facility to service the needs of the hospital as soon as possible after an event, yet also far enough away not to be impacted by the same regional event.

Hot sites designed to recover businesses far away from their original place of business are generally ill suited for health care institutions—unless the institution can afford to make everything highly available to a remote worksite near the disaster-impacted area.

Technologies such as Citrix, VMware and HP Storage Solutions, to name but a few, are important for the most critical systems, while lower criticality systems can be recovered as needed using tape backups and drop-shipped hardware. A smart approach to tiering applications will save money and ensure that staff is focused on the most important clinical and business data first, leaving less critical systems to be recovered later.

Choose the second site out of harm’s way, but near enough to the primary care facility to service patients quickly.

Partner with companies that understand health care & leverage disaster recovery off of new solutions.

---

### **Re:Think...**

the process. Are you talking to the right people in the company? Have we properly given them plans for business continuity and disaster recovery and explained the difference? Do they know what is at risk? Do clients have enough information to make good decisions?

---

## Contact

---

Kevin Burton

kevin@thinkbam.com

480.239.9724

---

Angela McGee

angela@thinkbam.com

480.239.5647