Continuity of Business: Does Your Hospital Have a Plan?

S Keene, L Auger

Citation

S Keene, L Auger. *Continuity of Business: Does Your Hospital Have a Plan?*. The Internet Journal of World Health and Societal Politics. 2006 Volume 4 Number 2.

Abstract

The Continuity of Business is vital in any setting and even more so in hospitals where the product is literally life and death. Considering the importance of the work that is carried on in hospitals all over the world and how this particular field is important and vital to almost everyone in the world, it only stands to reason that we all be interested in how the hospitals plan on continuing to care for the sick and injured in the event of a natural or man-made disaster. Continuity of Business requires thoughtful planning, setup, reaction, and follow through to ensure everything runs as according to plan even if the world around the hospital is completely out of control, it is reassuring that the hospitals that your very life depends on have complete control of their environments.

INTRODUCTION

Emergency is defined as a sudden, unexpected event requiring immediate action due to the potential threat to health and safety, the environment, or property. It is an extraordinary situation in which people are unable to meet their basic survival needs, or there are serious and immediate threats to human life and well being. What would happen if you woke up at 3 am with severe chest pains and numbness in your limbs but the area hospitals were closed due to flu pandemic? What would happen if you were scheduled for surgery but the computer containing patient records was down due to a computer virus? Fortunately for everyone the Hospital staff knows what to do. The hospital has a procedure response for both internal and external disaster situations. There is a template that the hospitals should follow and it can be used by any hospital. The make of the template is Business Impact Analysis (BIA), Risk Assessment, Selecting and Implementing Recovery Strategies, Contingency Program Policy & Standards, Hospital Data Backup and Storage Plan, Hospital Disaster Recovery Plan (DRP), Hospital Business Continuity Plan (BCP), Hospital Emergency Mode Operation Plan (EMOP), Hospital DRP & BCP Testing and Revision Plan.

REVIEW OF THE LITERATURE

What constitutes a disaster? Disasters can be man-made or natural. Natural disasters include floods, hurricanes, tornadoes, earthquakes, volcanoes, wild-land fires, thunderstorms and lightning strikes. (Sandhu 2002). Man-made can include terrorist, bio-threats, acts of war, and riots, explosions, train wrecks, chemical spills, and toxic waste spills, mining accidents and shipwrecks. Blackouts and Brownouts are also apart of the disasters that could occur. The effect of any of the above mentioned disasters on a hospital system could potentially be devastating. New Orleans for Example, The patients were moved after the threat had occurred, what a hospital should strive for is moving before the event or be self sustaining like the hospitals in Denver, Co. The experience with Hurricanes Katrina and Rita shows that critical emergency management capabilities must be ramped up from the minimum disaster management levels. When catastrophic disaster occurs, significantly more capabilities in relation with quantity and quality are needed.

Business Continuity Management is broadly defined as the process that seeks to ensure organizations are capable of withstanding any disruption to normal functioning. (Elliott, Swartz 2002). Medical facilities have become increasingly dependant on information technology services; this also renders the hospital venerable to equipment failure. Whenever a business is heavily dependent on information technology all risks and threats need to be considered when preparing for recovery. If disaster strikes and you cannot recover fast enough the consequences could be devastating. Unfortunately in the area of information technology you have another area to consider and be ever mindful of disgruntled employees and add that to the mix of natural and man-made disasters. The Continuity of Business plan for

information technology needs to include servers, storage, networking equipment and connectivity links as well as air-condition and power supplies. The Plan should ensure continued availability, reliability, and recoverability of resources. It should balance the costs of risk management with the opportunity cost of not taking action in preparing for disasters. The continuity plan should provide an enterprise-wide risk-based approach, covering People, Processes, Technology and Extended Enterprise to ensure continuing availability of business support systems and minimize disruption risks.

Disasters and downtime can affect all aspects of business including facilities, workers, communications, logistics and data. Many businesses in the United States have put a contingency plan into place; it's called Continuity of Business Plan. Continuity of Business is a back-up plan to ensure business as usual in the event of a natural or man-made disaster. A hospital is a business in every way; the only difference is its product. The patient. The processes and procedures a hospital puts into place to avoid mission-critical business interruption or data loss during any type of disaster is essential to ensure that the right fail over mechanisms are in place to continue operations. These fail over systems are often in geographically dispersed locations, so that data access can continue uninterrupted if one location is disabled. Systems and applications that can be impacted include electronic medical records, order entry, patient accounting, radiology/imaging services, reports and distribution workflow. Emergency care, Care Manager, patient Monitoring, Clinical profile, lab Dictaphone, Physicians portals, medical supplies and a variety of other applications. Some areas of consideration in information technology to keep in mind when establishing a Continuity of Business Plan are Performance: How is the application going to perform when you have to go beyond a data center over the WAN? Extended Distance: how far can you go? What is the impact of distance on my existing applications? Management of the Separate Data Centers: How do you manage a remote data center? The Complexity of Design and Deployment: What are the various types of Business Continuity and disaster recovery applications? Cost: Do you deploy a separate business continuity and disaster recovery for each? Availability: If one applications goes down it may impact others? What happens if the WAN goes down? What are the points of failure? Will the plan scale to future requirements? Security: What are the potential security threats created by the business continuity and disaster recovery plans that are in place? How do you preserve the integrity and privacy of the data?

El Camino Hospital in California has began an aggressive disaster recovery strategy with is new backup site in Southern California. It has also built a new hospital infrastructure that is seismic-tolerant. (Higgins 2005). The motto is No Single Point of Failure and they have spent $300 million dollars to build the complex and a separate disaster recovery site. The 400 bed nonprofit hospital is one of the most leading edge facilities of its kind. El Camino is the first hospital in the world to automate order entry for the physicians, and the smart hospital uses tablet personal computers and Bluetooth wireless technology for transmitting patient's vital signs, digital imaging for radiology and electronic charting to let the Doctors study test results and sign records from home using an SSL VPN. The goal of El Camino is to reach 99.9 percent up time for the information technology operations. In This particular area of the country Earthquakes are of considerable concern, El Camino is just a mere three miles from the massive San Andreas fault and it is even closer to the McArthur fault line and the new facilities that is slated to open in 2008 has been designed to meet California's aggressive earthquake preparedness law, which requires all newly erected healthcare facilities to be seismically tolerant. Part of the project includes an over $5 million data center. The hospital is currently testing the failover process between the two data centers. Some failovers are automatic while others are manual. The exchange servers are in standby mode and ready to be imaged with whatever server may go down, it takes less than an hour to get the servers back up and running. So if El Camino Hospital's complex network of water pipes were to burst in the event of an earthquake the failover system would automatically reroute an application from server A to server B at the Irvine site. Not all hospitals have the resources to encompass this approach; however there are several less expensive and aggressive ways to prepare for disasters.

When you began initiating business continuity into a health care system, you must keep in mind that the patients come first. (Patterson, 2000). At the very core of every hospital is the basic desire to take care of the sick and injured that walk through their doors. In order to perform this basic service every hospital must be prepared to assist the public regardless of the circumstances. In a disaster for hospitals the primary focus lies in lifesaving care. (Devlen 2000). The hospital is there to provide care during the patient's time of need and if you can not get to your local hospital then is

reassuring to know that the hospital has a backup plan. The back up plan is called the Continuity of Business Plan and it serves to assure that hospitals will be prepared to react, respond, restore and resume normal functions in the wake of a crisis.

The reason of the Continuity of Business Plan is to identify the most critical information needs for patient care, treatment, services, business processes and the impact on the hospital if information systems were severely disrupted. (JCR 2006). The sick and injured need a place to be treated regardless of the events happening around them. Another aspect you need to consider in implementing a Continuity of business plan is training. Plans cannot be considered reliable until they are exercised and have proved to be workable. Exercising should involve: validating plans; rehearsing key staff; and testing systems which are relied upon to deliver resilience (e.g. uninterrupted power supply). The frequency of exercises will depend on the organisation, but should take into account the rate of change to the organisation or risk profile, and outcomes of previous exercises if particular weaknesses have been identified and changes made. There is a need to train those responsible for implementing BCM, those responsible for acting in the event of disruption and those who will be impacted by the plans. This training and awareness can be elivered in many ways. Those involved in implementing BCM may require extensive training, whereas those with no direct responsibility may simply need to be made aware. Training should be updated whenever there are staff changes, changes in organizational structure, details in suppliers or contractors. Over the past several years different approaches have been taken to develop a fully functuional disaster recovery plan, one hospital in particular brought in a variety of vendors to assist with the development of the Continuity of Business Plan. The final plan had not been tested appropriatley nor had it been implemented to provide the hospital with the plan they needed in the event of a disaster, there was no major emphasis on refining the plan or any furthur development of the plan to accomidatethe changing threats that are inevitable, then the hospital had a disaster, a water pipe located above their main medical records system burst. This event forced the hospital to reexamine and complete an appropriate disaster recovery plan for every consivable event that could occur.

Crises will inevitably occur. Whether they are physical, such as an earthquake or a terrorist attack, or cyber, such as a distributed denial of service (DDoS), preparedness is the key to effectively managing a crisis. The difference between falling victim to an event and working through a highly challenging time is planning. (Paguet, Saxe 2005). New threats appear everyday, for example the avian flu threat. Is the avian flu threat real or hype? It is different from any other threat? What are the implications if the avian flu does become a pandemic? How can we prepare for it? So far the threat is restricted to people working daily and intensely in the avian industry. What if this particular strain of flu mutates and becomes increasingly transferable to humans and then results in an outbreak, which may spread across the world. What impact would that have on the hospitals that we depend on? Once an infection is discovered and its human-to-human or animal to human link is proven, then the plan must consider that the hospitals will be impacted. Will the doctors and nurses that are attempting to treat the outbreaks be affected by the symptoms?

Some key terms used in a hospital Continuity of Business Plan are Disaster POD (Point of Delivery). The hospital or health care facility that has been designated to support disaster situations in a specific geographic location. (Kirvan 2004). Some more terms to consider in understanding a hospitals continuity of business are Packaged Disaster hospital, which is a unit of sufficient medical supplies and equipment to establish a 200 bed hospital and these packaged disaster hospitals are placed through out the United States and overseas and are designed for long-term storage in order to enhance medical facilities in the event of a major disaster. Salvage and Restoration it the process of reclaiming or refurbishing computer hardware, vital records and office facilities following a disaster. The Associate hospitals are the hospitals that participate in the approved Emergency system that fulfills the same clinical communication requirements as a resource hospital. They have neither the primary responsibility for conducting training programs nor the responsibility for the overall operation of the emergency programs. Another key term to consider is Epidemic, it is the occurrence in a community or region of cases of an illness, specific health related behavior, or any other health related events that are clearly above normal expectancy, The number of cases that indicate the presence of an epidemic vary according to the agent, size, and type of population. The purpose of this is to identify epidemics as early as possible so that effective control measures can be put in place. It is also necessary to determine a disease that is only present for a limited time in a human or animal population that can be transmittable to humans and has a very high morbidity rate, for example the plague. Some areas to consider when implementing a plan of

action are Behavioral Epidemic, Disease Epidemic, Endemic, Pandemic, and threatened Epidemic.

Risk is defined as the potential of something occurring. Some risks can be reduced to the point of elimination, for instance a hospital can install a back-up generator system with the goal of ensuring 100% electrical availability. This helps protect the hospital from blackouts and brownouts. (Wallace, Webber 2004). What happens if the generator fails? What is the back-up plan for the back up and how does the hospital deal with it?

Healthcare organizations have long planned to minimize disruptions of materials by stockpiling key items to include medicines, sterile equipment, and disinfecants. Supplies are kept at the care units, as well as in central supply and storage that is readily accessible to a varied number of employees. In addition, reorder thresholds are set and procedures established to ensure the continued flow of materials to meet the needs of patients and medical staff. Business continuity planning is similar in that the goal is to minimize disruptions in automated systems by regularly stockpiling key information, essential equipment, and replacement parts. (Hoopinzarner, Luecke 1993) The broadening of Business Continuity shows that there is an underlying assumption that crisis incidents or business interruptions are systematic in nature, made up of both social and technical elements. (Elliot, Herbane, & Swartz 2002). Hospitals are now considering that even blow fuses after a power outage can affect Continuity of Business and they are planning accordingly. Backup generators have their own area of the plan as well as the avian flu. Every area that affects human life is a part of the Contingency plan. The backup locations are geographically separated to ensure that data is not corrupted and the backup hospitals are close enough not to seriously impact the health of the people being transported out of the disaster location to the recovery location.

CONCLUSION

The hospital in El Camino California is preparing for the future. A hospital was forced to reconsider it's Continuity of business plan after a water pipe burst and destroyed all of the medical records in the room below it. Threats to the hospital's Continuity of Business come from various sources and the threats change daily and yearly. The hospital is well advised to consider every aspect from a swarm of bees to a shipwreck in the ocean when planning for their disaster recovery. Information Technology continues to become more and more integrated through the daily operations of the hospital and is also an valuable source of consideration in the Continuity of Business Planning. If the system crashes because of a flood or earthquake or because a disgruntled employee launches a virus in the system, it is vital for the hospital to recover and continue its everyday functions. A well-organized disaster recovery plan will directly affect the recovery capabilities of the organization. The contents of the plan should follow a logical sequence and be written in a standard and understandable format. Effective documentation and procedures are extremely important in a disaster recovery plan. Considerable effort and time are necessary to develop a plan but the end results make all the difference in the world in the wake of a disaster.

References

r-0. Elliott, Dominic and Swartz, Ethnec. Business Continuity Management Routlegde, Taylor & Francis Group 2002.
r-1. Patterson, Kathy Lee. Business Continuity Management Briefing. 2000.
r-2. Develn, Angela. BCM & Risk Management Briefing. 2000.
r-3. Joint Commission Resources, 2006.
r-4. Paquet, Cathrine and Saxe, Warren. Cisco Press 2005.
r-5. Wallace, Michael and Webber, Lawerence. The Disaster Recovery Handbook. AMACON Div American Mgmt Assn. 2004.
r-6. Sandhu, Roopendra Jeet. Disaster Recovery Planning. Premier Press. 2002.
r-7. Kirvan, Paul. The CPM Dictionary: The single dource for Acronyms, terms, and Abbreviations in Business. Witter Publishing Corp. 2004.
r-8. Hoopinzarner, Cindy and Luecke, Randall. Healthcare Financial Management. 1993.
r-9. Elliott, Dominic; Herbane, Brahim; and Swartz, Ethnec. Business Continuity Management: A Crisis management approach. Routledge 2002.
r-10. Higgins, Kelly Jackson. Silicon Valley Hospital's RX for Business Continuity. Oct 27, 2005

Author Information

Shane Keene, MBA, MS, RRT-NPS, CPFT, RPSGT
East Tennessee State University

Lois Auger
East Tennessee State University