CareGroup Case Study

Sharon C. Perelman

Northwestern University School of Continuing Studies

Health Care Operations

404

Jay Anderson

November 1, 2011

CareGroup Case Study

In order to be properly prepared for an outage in the magnitude of what transpired to the CareGroup network, systems and process control may have prevented this unfortunate event from occurring. Instituting a preventive approach to network functionality and security, along with a contingency plan to deal with failures or breaches to the system should have been in place.

To start, an adequate IT budget meeting Benchmarks should be included in the strategic plan for the health care organization. This would allow for proactive upgrades, maintenance and support. It was clear from exhibits that CareGroups expenditures were lower than comparable organizations and established benchmarks. A committee in the IT department will evaluate request that influence the network in any way, including new equipment. No one person or single point of failure will be allowed in the system. The committee will make the final determination if, how and when any changes are made the potentially could effect the network, will be implemented.

Although the issue in this particular case was an unintentional breach causing a massive network failure, the institutions needs to aggressively deal with security. The cause of this could have been a cyber attack of even a disgruntled employee compromising the system. Thus a robust security protocol must be in place beginning with a complete security risk assessment. Physical security would include limited access to servers, equipment maintained in locked rooms, minimizing access to the network, and a secure login in with passwords. Adequate firewalls should be installed along with antivirus software at the user end that is updated and maintained. The physical hardware of the network must be continually monitored and maintained.

A clearly defined Contingency Plan to deal with emergencies correctly and efficiently will be in place. Defined conditions that will initiate the implementation of the plan will be identified. A contingency plan leader will be in charge once the process is started. The contingency plan will include levels of acuity such as green, yellow, red; each has protocols and steps to be taken. These protocols will be hospital wide and departmental. A system of reverting to a paper based charts, etc will be in place, this will include protocols and processes of how to implement the system down to the location of the paper material and sample charts that are pre-made. There will be a protocol in place to determine when it is safe to return to the computer network and direction as to the process for going back online hospital wide and departmental. Critical areas will be re introduced in order of importance. Procedures will guide the department is transferring information back into the system.

Although the case study states that no significant harm came to patients, I believe that it is impractical to think that patient care was not affected. After the crisis was over the staff was asked to report adverse clinical events, twelve reports were filed; yet we do not know the magnitude of these events. Patient complaints were reviewed but we do not have that information either. Impact on patient care although subtle would include delay in diagnosis and treatment as of result of the outage. Lab delays occurred and x-rays were catapulted into the stone age of real film! The discrepancy in time for orders to be implemented may have been completely acceptable in the pre computer era but are quite different now.

Although the initial internal response to the outage did not solve the problem of the network failure, it would have been premature to call in the “Big Guns” so quickly. Since there was an existing contract for support and maintenance with Cisco, they should have been consulted from the get go. Overall I think that this would have been improved the timeline.

Once the network came backup the first time and Halamka realized that it was unpredictable he acted aggressively yet appropriately contacting Cisco to come and manage the problem.

References

McFarland, F. W., & Austin, R. D. (2005, August 11). CareGroup Case 9-303-097 [Case Study]. *The Harvard Business Review*.