Disaster recovery

The Admitting System Crashes Patricia Hampton Dr. Allen HSA315 August 24, 2011 Identify at least three steps that the CIO could have taken to reduce the likelihood of the system failure. The chief information officer is the executive who manages the IT department and leads the organization in their efforts to develop and advance IT strategies. The role of the CIO in health care organizations is to: set visions and strategies, integrate information technology for business success, and make changes when necessary, build technological confidence, partner with customers, ensure information technology talent, and build networks and community.

They should also establish and maintain good working relationships with the members of the organization’s leadership team and communicate IT performance. It is the CIO’s job to manage and led the IT department to achieve organizational excellence and success (Wager, Lee, & Glaser, 2009). When it comes to the disaster recovery case study, three steps the CIO could have taken to reduce the likelihood of the system failure are; risk analysis, risk management lead by the chief security officer, and security system evaluation.

These three activities are part of the organizations administrative safeguards that can be used to improve the HCO’s information security program (Wager, Lee, & Glaser, 2009). Risk analysis and management process has eight steps; boundary definition, vulnerability identification, security control analysis, risk likelihood determination, impact analysis, risk determination, and security control recommendations. Through the risk analysis, policies and procedure are developed and a security risk management program is

put in place. The CSO, chief security officer, is in charge if administering and managing the program.

Security system evaluations should be periodically performed, by the CSO, to evaluate the risk currently no adopted technical security standards designed for health care information systems, which makes security evaluations difficult. The International Organization for Standardization (ISO) has developed general standards for security techniques, which allows HCO's to use a common set of requirements to compare independent security evaluation results. The CIO is ultimately in charge of managing and leading the IT team to perform the risk analysis, risk management, and security evaluation processes (Wager, Lee, & Glaser, 2009).

What plans and changes could JRMC make to reduce the likelihood of a future system failure? JRMC implemented their current system, TechMed, in 1995 and they are concerned about the fragility of the application because the technology is obsolete. They are in the process of replacing the TechMed system in two years, but with the recent system failure they may want to change the date. It would be wise for JRMC to replace the system as soon as possible to help prevent further operational problems. They should also make sure they hold security awareness and training programs for all employees.

The training should include periodic security reminders and address protection from malicious software, log in monitoring, and password management. They should perform information system activity reviews that periodically check records of information system activity, such as audit logs,

access reports, and security incident tracking reports (Wager, Lee, & Glaser, 2009). JRMC should have a contingency plan in place that address the data backup plan, disaster recovery plan, emergency mode operation plan, testing and revision procedures, and applications and data criticality analysis.

There should be a process for allowing facility access to support the restoration of lost data under the disaster recovery plan and emergency mode operation plan. A facility security plan should also be in place to safeguard the facility and its equipment from unauthorized access, tampering, and theft. These are just a few changes that JRMC could make to help reduce the likelihood of future system failure (Wager, Lee, & Glaser, 2009). Another key change that JRMC could make is having a viable backup copy of the database.

This would help the organization if failure were to occur again and also save them from performing a full database recovery. What factors did the Root Cause analysis reveal that contributed to the system failure problem? First, root cause analysis (RCA) is a problem solving method used to identify the root cause of a problem or event. The practice is believed to work best when attempting to address, correct, or eliminate root causes as opposed to simple addressing the immediate symptoms.

By identifying the root cause of a problem, it can create effective corrective actions that can possible prevent that problem from ever recurring. The analysis is performed after the event or problem occurs, but it can also be used as a pro-active method (Bellinger, 2004). As stated in the case study,

JRMC had a scheduled performance test being done on December 20, which caused them to take down the link between the main data center and the disaster recovery center. This is a routine test that should not cause any problems, but on December 21, JRMC lost power to the disaster recovery center.

Emergency power was instantly put in place to get the disaster recovery center up and running. Losing power to the disaster recovery center is not good because the disaster recovery center is what the organization uses if the main data center goes down. As a precaution, a backup was performed on the TechMed data base and shortly after the system became sluggish and unresponsive. They discovered that there was corruption in the data base and in the backup performed. The problem could have started with the performance testing, the power outage, or the backup performed.

The root cause analysis will investigate and determine which of these problems the main cause of the system failure was, and the IT team will try to resolve the problem so that system failure doe not continue to occur. What were the factors likely contributing to the system failure? As stated in the case study, JRMC was conducting a routine performance test on their system on December 20, and the link between the main data center and the disaster recovery center was taken down. On December 21, power was lost to the disaster recovery, but emergency power was immediately put in place.

The problem here was the link to the disaster recovery center had not been restored following the performance testing. As a precaution, a backup was

performed on the TechMed database. Shortly after the backup was performed, the system became sluggish and unresponsive. The case study states, that corruption was discovered and the backup performed was also corrupt. These are all of the factors leading up to and post system failure. The key is performing a root cause analysis immediately after the event to determine which of these factors could have been the main cause, so that JRMC can prevent system failure from reoccurring.

What appeared to be most important factors contributing to the system failure? One important factor contributing to the system failure was the loss of power to the disaster recovery center. Also, the backup performed on the TechMed database system. Another key factor is that after the performance testing was conducted, the power to the disaster recovery center was not restored. This may have helped prevent the corruption from occurring. The corruption to the database system is the other important factor that may have contributed to the system failure.

Data corruption occurs as a result of an external agent deteriorating the computer database. Some examples of external agents are; viruses, flaws and failures, hardware and software incompatibilities, and environmental threats like power outages, weather, dust, and extreme temperatures (Wager, Lee, & Glaser, 2009) As a board of trustee member what questions would you ask the CIO? There are many questions a board of trustee member would want to ask the CIO regarding the system failure. How effective is JRMC’s governance system? Are the IT strategies well aligned with JRMC’s overall strategic goals?

Is JRMC’s CIO actively involved in strategy discussions? Does JRMC’s senior leadership discuss IT agenda items on a regular basis? Does JRMC perform regular audit trails and where are the records kept? Audit trails are important because they record who has access the system and the operations they performed during a given time period. They are generated by specialized software and have multiple uses in securing information systems (Wager, Lee, & Glaser, 2009). Other questions a board of trustee’s member may want to ask are; is the infrastructure checked regularly?

Was fire wall protection installed? Why was there no viable backup copy of the database? These questions would be asked to ensure that the IT team is checking the infrastructure to see if the systems are reliable. To see what the overall security of JRMC’s health care information is and to find out why they had no backup copy of their database, especially since the system was obsolete. What issues and problems should a disaster recovery plan cover and prepare for? A disaster recovery plan should clearly map out the process of continuing normal business operations and salvaging vital data and equipment.

It should act as a guide on what to do during and after a disaster for the various teams in the organization. First, backup files must exists and they organization should have copies of them. Where you store your backup may be just as critical as creating the backup. Backup files should be saved and stored on another network drive or separate hard disk. It is also important to have your backups available away from your production site. It is very important to have a recovery committee should be in place and consist of

members of; the management team, risk management, data management, security and IT team.

There should be a complete contact list of the members on the committee and alternate contact information. The plan should clearly state what defines a disaster an address minor as well as major disasters. There should be employee training for the skills needed in the salvaging and resuming phases during and after the event. A list of functions that are critical for business continuity. Contact details of fire department, police, ambulance and floor plans and blueprint of the building should be readily available (Shimonski, 2004).

How does an organization determine the amount to spend to reduce the occurrence and severity of such episodes? One of the primary challenges health care organizations face when developing an effective security program is balancing the need for security with the cost of security (Wager, Lee, & Glaser, 2009). It is very difficult for health care organizations to calculate the likelihood of; human threats, natural and environmental threats, and technology malfunctions. It is also hard to determine how much damage they may have on the organizations information systems.

This makes it hard for any health care organization to know how much to spend on security to remove or reduce the risk (Wager, Lee, & Glaser, 2009). What we do know is that having a disaster recovery plan is crucial and the organization must have approval from the CIO for development and implementation of the plan. We also know that contingency plans, data backup plans, disaster recovery plans, and emergency mode operation plans

are required under the HIPAA security rule and the organization must be able to provide funding for developing them (Wager, Lee, & Glaser, 2009).

References Bellinger, G. (2004). Root cause analysis. Retrieved on August 16, 2011 from http://systems-thinking. org/rca/rootca. htm. Shimonski, R. (2009). High availability: disaster recovery planning. Retrieved on August 17, 2011 from http://www. windowsnetworking. com/articles_tutorials/High-Availablity-Disaster-Recovery-Planning. html. Wager, K. A. , Lee, F. W. , & Glaser, J. P. (2009). Healthcare information systems: A practical approach for health care management (2nd ed.). San Francisco: Jossey-Bass.