IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP4402

INFORMATION SYSTEM FAILURES IN HEALTH CARE ORGANIZATIONS:

CASE STUDY OF A ROOT CAUSE ANALYSIS

Pamela E. Paustian, MSM, Health Policy and Outcomes Research, School of Public Health, University of Alabama at Birmingham, Birmingham, AL 35294, paustian@uab.edu; Donna J. Slovensky, PhD (Contact Author), Division of Management and Information Sciences, School of Health Related Professions, University of Alabama at Birmingham, Birmingham, AL 35294, (205) 934-1679, donnaslo@uab.edu; Jacqueline W. Kennedy, MPH, Division of Management and Information Sciences, School of Health Related Professions, University of Alabama at Birmingham, Birmingham, AL 35294

ABSTRACT

Preparedness for response and continued operation of a health care facility following an information systems disaster must encompass two facets: continuation of patient care delivery and continuation of business processes. This paper reports a root cause analysis following an information system failure that compromised the organization's ability to capture clinical documentation for a 33-hour period.

INTRODUCTION

Delivery of health care is an information-intensive process, and the technology associated with data capture and information management is a critical operational and strategic resource. Most HCOs prepare formalized plans, policies, and procedures for recovery of computerized information system (IS) functionality and the recovery of any lost data following an IS disaster. Unfortunately, many disaster recovery plans are inadequate to guide action when a disaster occurs for a number of reasons. Conducting a root cause analysis in the aftermath of an IS disaster can be an important first step in evaluating the adequacy of existing recovery plans.

DEFINING DISASTER

In general usage, the term 'disaster' describes an adverse event that occurs suddenly and unexpectedly. Terminology used to describe disasters within a specific context may incorporate several generic definitions to explain the contextual usage. Morris (1990) defined an automation-related disaster in a health care organization as "any situation that results in an automation support outage of sufficient duration to significantly disrupt hospital business and/or clinical services." This broad definition permits organization prerogative in designating the scope of information system disaster preparedness. This prerogative is not trivial as information systems in HCOs are both complex and dynamic. Information executives must make purposeful decisions about the time and financial resources expended to prepare and maintain disaster recovery plans – plans they hope never to implement. The degree of risk an organization accepts must be based on educated judgment about the likelihood given events will occur and the liability associated with failure to prepare for the eventuality.

INCENTIVES FOR IS DISASTER RECOVERY PLANNING

For hospitals, external disasters affecting the geographic market area served actually may increase the need to provide health care services. When the physical resources of the facility are compromised by environmental conditions, such as wind and water damage from a hurricane, delivery of care may become particularly challenging. Planning for and recovery from disasters, therefore, is mission-critical to HCOs. As HCOs are rapidly increasing their dependence on digital information capture and real-time data analysis to provide patient care, "protection of mission-critical information technology … is gaining serious attention" (Bandyopadhyay & Schkade, 2000).

The delivery of health services is information intensive and information dependent – from both clinical and business management perspectives. Loss of all or a portion of IS functionality quickly compromises clinical and business processes, and information is recognized as a key strategic resource in health care organizations (Kelly, 2000). Loss of stored data and information can have far-reaching effects, potentially including patient injury, legal liability, and significant financial loss to the organization. In short, the health care industry has become dependent on information technology to conduct its business – delivery of clinical care. Anticipating and preparing for management of and recovery from information system disasters is as mission-critical for health care organizations as is preparing for continuation of patient care in the event a disaster occurs. Determining the underlying cause of IS failure is a pivotal factor in assessing the adequacy of recovery plans. Root cause analysis, which is directed specifically at finding the underlying cause, is an appropriate analytical model to employ. Thus, omitted or inadequate documentation in the disaster recovery plan can be improved.

EXTERNAL REGULATORY REQUIREMENTS

Several regulatory agents and some legislative acts compel health care organizations (HCOs) to have formalized disaster recovery plans. For example, hospitals seeking accreditation from the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) must show evidence of compliance with published standards, which include disaster planning and protection of information resources. The Health Insurance Portability and Accountability Act (HIPPA) of 1996, potentially the most intrusive legislation affecting health care organizations in the past decade, incorporates many regulations specific to information resources.

INFORMATION SYSTEMS FAILURE

Information systems fail for many reasons, relatively few of which are attributable specifically to defects in system hardware or software. Although operational failures occur with some frequency, the length of downtime and operational impact usually are much less severe than failures due to disaster occurrences. Therefore, planning to avoid system damage or data loss and recovery in

This paper appears in *Managing Information Technology in a Global Economy*, the proceedings of the Information Resources Management Association International Conference.

the event of damage or loss is focused on likely events of significant magnitude. It is important to prevent bad things from happening to good data, particularly when data loss or corruption can result in legal or financial liability.

Categorization of more than 5,000 computer outage incidents between 1982 and 1994 revealed that 47.1% of those outages resulted from events that would be classified as internal or external disasters. Another 27.7% were caused by power outages (Williamson, 1995). According to Robertson's (1997) findings, each online outage averaged 4 hours and cost companies an average of $329,000 in lost revenues and productivity, with 355 worker hours being lost for each hour of unscheduled downtime. Most HCOs are reluctant to report events resulting in negative impacts on patient care for liability reasons. Therefore, data quantifying the cost of information system outages relative to patient care are difficult to investigate.

CASE STUDY

This study was conducted as an investigation of a single case. A single case study is a desirable alternative to investigating multiple cases when the single case is critical, extreme or unique, or when it offers access to previously inaccessible scientific observation (Yin, 1994). The information available at the site was rich in detail not reported in current literature. A sampling strategy whereby the case site is selected because it is a "typical case" (Patton, 1990) was particularly appropriate for this investigation because extreme cases – those which were unsuccessful and those which offer solutions so unique they cannot be replicated – are of little use to instruct other managers or as a foundation to formulate testable hypotheses for future research. While each information outage is unique, the root cause analysis methodology can be applied in many situations (Spath, 1997).

ESCRIPTION OF THE INCIDENT

In August 2000, what should have been a standard, two-hour, information system upgrade in a Southeastern hospital turned into a 33-hour information disaster. The 300-bed hospital is the primary element of a multi-focus delivery system that provides technologically advanced health care in a competitive metropolitan market. Most clinical data are captured electronically at the point of service.

The enterprise-wide information system is configured as a sophisticated network of servers and PC workstations and terminals. Historically, the hospital employed a "best of breed" approach to applications development. Therefore, multiple vendors are represented among the clinical, administrative, and decision support systems. This type of IS structure requires collaborative relationships among vendors to develop interfaces between legacy systems and the emerging data repository. The primary vendor has been designated as responsible for communicating with other application and hardware vendors during system upgrades or new installs.

Events Leading to the IS Disaster

The primary vendor of the main information system was brought on-site to perform a minor hardware upgrade on a clinical documentation system. During the upgrade, the technicians determined that the hardware firmware would have to be updated to support the new hardware changes being made. After verifying that a good system backup existed for the server, the vendor identified the required firmware version and downloaded the patches to the system. From the time of this action, the chain reaction that followed was non-preventable. The re-start of the system after the firmware update failed. The information system supporting clinical documentation for the entire hospital failed and was down.

RECOVERY ACTIONS TAKEN

Procedures specified in the hospital's IS Disaster Recovery Plan were implemented. Hospital Information System (HIS) Department employees specified in the procedures manual were contacted to resolve the problem. HIS employees worked with the application and hardware vendors to evaluate the system status and to determine the extent of the recovery be required. The decision was made to attempt a quick recovery using the customized recovery tape created monthly.

Five hours after beginning this "quick" restoration, the system re-boot again failed. Further investigation by HIS personnel revealed that this version of recovery software had a known bug that sometimes created restoration tapes that were corrupted. Although aware the bug existed, the vendor had not installed the patch designed to fix the bug. The hospital had no knowledge that the bug existed. The vendor's failure to maintain the system properly prevented system recovery by restoring from a backup.

Ten hours from the occurrence of the disaster event, the HIS staff and supporting vendors determined that a complete system rebuild would be required. This would include operating system, database server installation, application interface installation, and data recovery from backup tape. The rebuild process required 23 clock hours to have the system up and functioning properly.

ROOT CAUSE ANALYIS

After recovery of the system failure, the IS manager initiated a formal analysis of the events that occurred and the responses taken to determine the root cause of the event and whether the root cause could be eliminated or minimized. A secondary goal was to determine whether existing procedures provided adequate guidance to investigate and manage the situation, and to identify any necessary revisions to the recovery plan documents.

FINDINGS

The lack of adequate communication among the vendor groups supporting various elements of the organization's system was identified as the root cause. Instead of direct vendor-to-vendor communication, HIS employees (who had no knowledge of the bug) talked with the vendors separately and communicated information to the vendors. Without direct communication between the individuals most knowledgeable about the technical details of the system hardware and software, what was expected to be a simple two-hour hardware upgrade turned into a disaster.

The existing IS disaster recovery plan was implemented, but the plan did not contain a tested procedure specific to the type of disaster that occurred. Appropriate procedures and personnel notifications had been followed prior to the upgrade and approvals to proceed were given. The vendor that upgraded the system was familiar with the organization's current IS setup and anticipated no trouble with the 'minor upgrade'. The hospital could not have anticipated the failure would occur. Therefore, the existing plan and procedures for disaster recovery were determined to be adequate. One additional policy was incorporated into the plan to clarify the tape pull procedure.

SUMMARY

An information systems problem of the magnitude described

in this case – 33 hours downtime – is commonly referred to as a disaster. The HIS department at this hospital not only responded to the systems problem and corrected it, they aggressively maximized the learning potential the event afforded by conducting a root cause analysis. In addition to identifying and correcting the communication problem between the vendors, several other important outcomes accrued from the post-event analysis. First, a previously existing bug in the information system was corrected. Second, the formal disaster recovery plan was improved by adding a policy regarding the tape pull procedure. Third, the hospital documented a successful test of the disaster recovery plan. Fourth, the manual clinical documentation procedures specified for use in the event of IS failure were tested and found to be adequate.

As organizations become more dependent on data communications networks and telecommunications, it is critical to be able to recover quickly from a disaster. The primary problem in this disaster was that inadequate communication occurred among the vendors involved in maintaining the information system. A professional audit, at least biennially, of all systems and vendors involved may be necessary to maintain the proper links of communication and to ensure the integrity of the disaster recovery plan.

Managers must attempt to avoid disasters by aggressively looking for weak areas within the recovery plan. Frequent testing and improvement of the recovery plan is more desirable than demonstrating a successful recovery in a disaster situation. A plan can become outdated in as little time as one business quarter, because of internal changes. Organizations cannot “afford to place their plans on the back burner” (Kelly, 2000).

* References available from contact author.