Chapter 73
Business Continuity and Disaster Recovery Considerations for Healthcare Technology

Edward M. Goldberg
Capella University, USA

ABSTRACT

As the healthcare industry moves towards adoption of electronic collection and storage of health data it becomes increasingly dependent on the successful functioning of these technologies in order to ensure access to this important information. This chapter explores the technical, ethical and legal issues associated with the importance of careful planning and implementation of robust disaster recovery procedures as well as the importance of business continuity activities in assuring that this data is available following a system failure or other event that may introduce risk of data loss.

INTRODUCTION

The Rationale for Contingency Planning to Protect Healthcare Technology

Traditional emphasis for protecting healthcare technology systems and the data they serve is focused on preventing data corruption, misappropriation and misuse of the information (Bandyopadhyay & Iyer, 2000). Due to resource constraints, the potential for the loss and/or unavailability of these systems is often overlooked and/or neglected. The past decade provided ample rationale for seeking to protect society's critical infrastructure from acts of terror, hurricanes, tsunamis, floods, etc. Healthcare technology is now an inextricable element in that infrastructure and preparing for such eventuality is arguably an ethical responsibility of those responsible.

DOI: 10.4018/978-1-4666-4707-7.ch073

Given the substantial reliance upon and critical nature of electronic health records, the focus on the security and ethical use of such information is appropriate (Ahlfeldt et al, 2009). The unit cost of storage and the systems which process and make that information useful generally decreases over time as for most such technology. The amount of storage needed has been growing exponentially for several years and will likely continue to do so for the foreseeable future. Similarly, the need for increased processing power to handle all of that information, periodic technology refreshes to keep pace with the computing environment in which the information exists as well as increased bandwidth and network capacity contribute to a substantial and ongoing cost. That cost and shrinking budgets in healthcare create a barrier to creating a resilient computing environment, thereby leaving these systems vulnerable to disasters and other major business interruptions.

Business Continuity and Disaster Recovery Defined

Business Continuity (BC) plans provide for the logistics, resources, infrastructure and strategies that allow an organization to perform its critical business processes during and after a disaster or other event that would otherwise cause the interruption or cessation of those processes (Goldberg, 2008; DRII, n.d.). These are plans that an organization uses to maintain the processes that it considers most important and necessary for its continued existence and ongoing viability. Typically, BC plans are designed to account for the loss of facilities, people and/or systems (any one of these or any combination of them). The details of the processes an organization must continue and how it does so vary widely, as do the risks and scenarios that could challenge its ability to perform effectively.

Disaster Recovery (DR) plans provide for the continuance or timely recovery of Information Technology (IT) systems. DR plans prioritize the work required to recovery computer systems, telecommunications systems, networks, data, etc., during and after a disaster or other disruptive event (Goldberg, 2008; DRII, n.d.). *DR plans are based upon BC plans.* Recall that BC plans account for loss of facilities, people and/or systems. The pervasive use of technology has embedded IT systems into many business processes. BC plans typically include *Recovery Time Objectives (RTO)* and *Recovery Point Objectives (RPO)* which define the timing and order by which the organization needs IT systems restored to be able to fulfill its BC planning objectives.

Specifying DR Needs: Recovery Time Objectives and Recovery Point Objectives

RTO is the time from when a disaster or other disruption disables an IT system until it is restored to service (Disaster Recovery Institute, n.d.). Faster recovery times generally require more expensive solutions than longer recovery times, so RTO is generally set to the longest time that the organization can practically continue without the system.

RPO is the point in time to which data restoration is made following a disaster or disruption (Disaster Recovery Institute, n.d.). While a 24 hour RTO means that a system will be available for use within 24 hours, a 24 hour RPO means that the data will be 24 hours old when the system is restored, and data after that point is not available. The criteria for establishing RPO for various IT systems varies by organization, and is typically a risk/cost/benefit analysis. For example, financial institutions typically have RPO of zero for their systems which are transaction-based because the loss of even one transaction could be very costly, disruptive and perhaps prohibited by regulation.

It is conceivable to have no data loss (RPO = 0) but still have an RTO that is not zero. Email systems are often so configured – when the system becomes available, all of the email from before the event as well as email that came in during the