Computer Crash — Lessons from a System Failure

Peter Kilbridge, M.D.

Although executives and physicians at the Beth Israel Deaconess Medical Center in Boston have had reason to take great pride in their advanced clinical computing system, they recently had a wake-up call when the system suffered a full-scale failure. Before the crash, the medical center's information-systems staff had designed and implemented a variety of applications to aid clinicians in caring for patients. With this system, clinicians throughout the medical center and the six affiliated CareGroup hospitals can gain access to laboratory results, radiographs, and electrocardiograms electronically, using a secure Internet browser. Patients also have secure access to their test results over the Internet. Since 2001, physicians at the medical center have been placing all inpatient orders through the system. Before Wednesday, November 13, 2002, many members of the current class of interns at the hospital had never written an order on paper.

On that date, a researcher at the hospital who was sharing data with colleagues inadvertently flooded the network with large quantities of data, causing it to slow drastically. The information-systems staff scrambled to solve the problem, flying in equipment and experts from the network vendor, Cisco Systems. These efforts resulted in a partial recovery of the system, but then it slowed down again. Twenty-four hours into the crisis, the decision was made to shut the network down and revert to manual processes throughout the hospital.

The outage lasted four days. During this time, hospital staff members from ward clerks to the chief executive officer hand-carried patient records, laboratory-test results, and countless other documents around the hospital in order to maintain clinical operations. The delivery of care continued; contrary to early reports, the emergency room remained open, and routine and emergency admissions and transfers continued at the usual volume. Chief information officer John Halamka talked early and openly with reporters about the outage, which received widespread coverage in the local and national media.

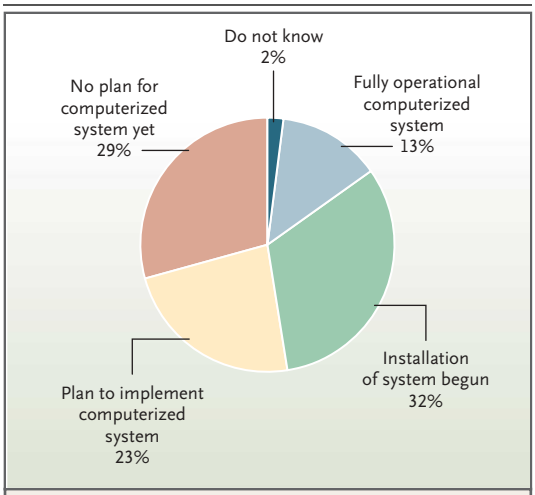
What should we learn from this event? Although some lessons can be drawn from specific aspects of the CareGroup experience, the increasing reliance of hospitals on information technology raises larger questions about the vulnerability of clinical and administrative operations to technological disruption. In the fall of 2002, the Beth Israel Deaconess Medical Center was operating an extended computer network designed to meet the requirements of a much simpler environment. In addition, some network equipment was old and needed to be replaced. The principal point of failure was a software program for directing traffic on the network. The program was overwhelmed by a combination of data volume and network complexity that exceeded the software's specifications. Once the network became dysfunctional, the diagnostic tools for managing it, which had to be used from within the network, were of no help.

All computing systems are vulnerable to a wide variety of potential threats. Viruses are a constant threat; new and more dangerous versions appear on the Internet daily, and they are capable of wreaking havoc in hospital systems. Internal "attacks" — whether unintentional, as in the Beth Israel Deaconess case, or malevolent — are particularly hard to guard against, since the attackers have legitimate access to the network. As a computer-system consultant to hospitals, I know that most hospitals have policies and procedures for the appropriate use of computer systems but that many users are unaware of or ignore them, usually with few or no consequences. The problem is amplified in academic medical centers, where researchers with independent sources of funding can purchase hardware and software independently of corporate oversight. Wireless network computing, which is being used increasingly in hospitals, is especially vulnerable to security breaches. In addition, "firewalls," which provide protection against unauthorized external access through the Internet, are far from perfect; a small percentage of attackers may be able to penetrate firewalls and gain access to internal systems.

Systems are available for managing a malfunctioning network such as that at the Beth Israel Dea-

coness Medical Center. "Out of bandwidth" management tools can be used to monitor the network without having to work from within it. Intrusion-detection systems identify sources of excessive data traffic and, if necessary, shut off access to the network. Although these systems have been available for several years, many hospitals have not yet adopted them.

The greater lesson concerns organizational responsibility. The events at the Beth Israel Deaconess Medical Center could have occurred at any of many medical centers in the United States today. Since the clinical computing systems at most hospitals are not as complex as those at Beth Israel Deaconess, the service disruptions might have been less severe. But there is a move toward the adoption of increasingly advanced clinical applications (see Figure), including computerized entry of orders by physicians, electronic records of drug administration, and online clinical documentation. Many of these applications have the potential to improve patient safety by reducing errors, particularly in the management of medications.



Use of Computerized Patient-Records Systems in U.S. Hospitals, According to Chief Information Officers.
Data are from the Healthcare Information and Management Systems Society, 13th Annual Leadership Survey Results, 2002.

As hospitals become increasingly dependent on information technology for clinical as well as financial operations, the responsibility to maintain and protect their information systems increases proportionately. This has been better understood in the financial sector, where organizations depend on their information systems for core operations. Many such organizations have learned that managing networks with the expectation of maintaining a continuous computing environment (i.e., no unscheduled downtime) is critical to their survival. Carrying out this responsibility requires an investment — financial and managerial — to install the right hardware and to manage the risks of the system.

It will be difficult and costly for hospitals to meet this challenge at a time of financial hardship throughout the industry. But the incident at the Beth Israel Deaconess Medical Center serves to remind us that computer systems are becoming critical to all aspects of hospital operations. There will always be risks, and costs of mitigating them. Hospital executives, boards, and information-systems departments must engage in an ongoing process of assessing the risks, costs, and benefits of information technology and structuring investment and management decisions accordingly. Technology that is critical to patient care must be managed as such.

From Kilbridge Associates, Cambridge, Mass.