

Healthcare IT Testing: A New Business Imperative for Health Systems

Authors
Mike Gibbs
Frances Dare

May 2008



Cisco Internet Business Solutions Group (IBSG)

Healthcare IT Testing: A New Business Imperative for Health Systems

Introduction

The healthcare industry is at a tipping point: a large number of hospitals are IT-enabled to the point where clinical care and business operations can become severely impacted when information technology fails. For the first time, hospitals and health systems must understand the impact of IT downtime and suboptimal performance—often referred to as IT degradation—on the delivery of care. For example, if a hospital's electronic health record, medication administration, and order entry systems are unavailable, physicians and clinicians would be hard-pressed to properly provide patient care.

According to HIMSS Analytics, 24.1 percent of U.S. healthcare organizations have reached Stage 3 adoption of electronic medical records (EMRs)—this means that clinical documentation, imaging, decision support, laboratory, and pharmacy systems are now IT-enabled. As more organizations approach Stages 4 and 5 of EMR adoption—where all orders for medical procedures, such as X-rays, lab tests, and medications, are entered electronically—the availability and optimal performance of Health Information Technology (HIT) becomes increasingly critical.

Despite the risks that may come from dependence on HIT, hospitals have neither recognized the need for HIT testing nor established the facilities and programs needed to understand, assess, and manage related risks. Research from the Cisco Internet Business Solutions Group (IBSG) indicates that very few hospitals have *any* systematic programs with which to test the resilience and stability of their HIT environments or to model the operational impact that different levels of degradation have on HIT.

Healthcare technology is complex. For example, hospitals and health systems have a large number of IT applications, stringent IT infrastructure requirements, many users (both on and offsite), and numerous IP-enabled biomedical devices from multiple vendors. With this much complexity, anything could go wrong. Assuming that an organization's IT systems will work properly without testing them first is like jumping out of an airplane without a parachute; therefore, it is important to understand that any failures in HIT can seriously impact both patient care and staff productivity.



Technology Performance Is a Business Problem, Not an IT Issue

A well-publicized HIT outage occurred at Beth Israel Deaconess Medical Center in Boston in 2002.^{1,2} A member of CareGroup Healthcare System, Beth Israel Deaconess relies heavily on IT to provide patient care and was not prepared when the network failed for three days due to degradations and outages. During the outage, medical staff had to revert to a paper-based system to order lab tests and results. This was a new experience for many; lab results that were previously available in 45 minutes took as long as five hours to process, and staff members—from ward clerks to executives—stepped away from their current roles to help transport paper records to and from the lab. The outage resulted in an unquantifiable loss in both revenue and expenses related to the additional staff needed to process paperwork and other documents manually.

While the incident at Beth Israel Deaconess was large in scale, an outage of this magnitude is not the norm. Outages on a smaller scale, however, do occur frequently in health systems. Unfortunately, the issue of IT availability is not often discussed in healthcare, and business leaders do not clearly understand the impact that degradation has on their organizations. Because of this, outages remain a clear and present danger. According to a 2005 research paper by Infonetics Research titled “The Cost of Enterprise Downtime: North American Vertical Markets,” the average healthcare organization experiences 180 hours of system outages and 212 hours of system degradation per year. Although this represents a mere 2 percent loss of IT availability, according to the report, the financial impact from the associated loss in staff productivity is significant.

How can healthcare leaders clearly measure the impact of IT degradation on their workforce? More important, how can health systems better assess IT resilience to support patient care and minimize outages and downtime?

IBSG developed a “downtime calculator” to help quantify the economic impact of network outages and degradations, particularly in the area of productivity costs. To estimate the cost of lost productivity annually, IBSG used a hypothetical example of a 5,000-employee hospital with IT at 99.9 percent availability, resulting in 180 hours of system degradation. Using the calculator, IBSG determined the loss to be nearly US\$3 million.

Hospitals face other, equally important risks beyond losses in productivity due to IT degradation. System downtime and outages may result in lost revenue if the hospital is forced to close certain services such as the emergency department, or reduce the availability of services such as elective surgeries and radiology tests. Degradation may also lead to poor patient care, raising legal concerns. If an outage creates significant operational challenges, it could jeopardize a hospital’s accreditation with organizations such as The Joint Commission, as well as its reputation with the public.

1. Mark Anderson, “Medical Grade Servers and the Effect of System Uptime for the Healthcare Industry,” 2007, AC Group.

2. Kilbridge, P., “Computer Crash—Lessons from a System Failure,” *New England Journal of Medicine*, March 6, 2003.

Clearly, hospitals and health systems must work to minimize system downtime and degradation. An effective strategy to help reduce risks associated with IT outages starts with a systematic, controlled method for testing applications, infrastructure, and emergency/contingency processes in a test laboratory. The advantage of a well-designed, properly staffed, permanent test lab is that it provides a platform on which the operational environment can be simulated accurately. Only a handful of health systems attempt anything close to this today; most rely—at their own peril—on application-specific testing services from IT vendors and consultants. The problem with relying on external partners to perform tests is that it creates a gap in the testing process.

Testing-Capability Gap

Before HIT testing can occur, it is important to understand the gap that exists between how vendors test their products and how the products are actually used in a hospital or health system. On one side of the gap is the hospital environment—most hospitals operate 24 hours a day, seven days a week and therefore have no window of opportunity in which to test hardware and software.

On the other side of the gap is the inability to test HIT systems in an integrated manner that reflects the hospital's technology environment. Most products are tested individually by vendors at their own facilities—a process called “individual product testing,” which involves testing software and hardware products in isolation. While this method is an effective way to test individual product performance and functionality, it fails to show compatibility issues with hardware or software, or what happens in an end-to-end customer environment. This means that business risks such as security breaches likely will go undetected. *(For additional examples of vendor IT tests and test methods, see Appendixes A and B.)*

Vendor tests may also miss many software defects and vulnerabilities. According to Gartner, Inc., in 2005, 60 percent of Web applications had an exploitable vulnerability such as buffer overflow attacks, where the attacker sends more information to the application's memory than has been allotted. A study from the eHealth Vulnerability Reporting Program (a consortium of healthcare industry leaders who address security vulnerabilities in HIT) found that organizations may be susceptible to a range of software vulnerabilities, for a long time—a period of 89–636 days was documented in one example.

The test labs allow hospitals and health systems to test HIT in an environment that meets, or mirrors, the unique conditions of their healthcare environments, not that of their vendors. There are five scenarios for which a test lab offers the ideal testing approach.

Penetration Testing (Ethical Hacking)

Penetration testing is the act of probing a computer system to find vulnerabilities an attacker could exploit. Healthcare organizations generally cannot perform penetration testing because the task requires the test engineer to “damage” the technology to find weaknesses; doing so is nearly impossible when IT is used by clinicians 24 hours a day, seven days a week. A well-designed penetration test performed in a test lab, however, can measure the degree—small or great—to which the organization is vulnerable to hackers.

System Resilience Testing

Healthcare systems and hospitals have a common concern: whether or not their technology systems meet their organization’s needs. Resilience testing shows how technology will behave in an information-overload or emergency situation, such as a mass casualty, and provides detailed information about system bottlenecks and a pathway to remediation.

Failure Testing

Failure testing demonstrates how the environment performs when specific equipment fails. Effective failure testing enables the organization to better understand how users will be impacted if, for example, the system is slow to respond to queries. Failure testing can help the organization remediate or create an effective plan to anticipate possible system failure.

Software Version and Patch Management

Controlling the number of software versions in use and managing software patches are key to an organization’s software strategy. Hospitals and health systems do not update software to resolve known security risks because their complex environments require significant testing prior to deployment. The test lab enables simple and effective testing of software patches or new software versions using the actual applications and devices that are available.

Application Certification

A lab can be the ideal environment in which to test new software, enabling healthcare organizations to certify their applications as being safe to use, and significantly decreasing any risks that may arise from adopting new technology.

Unfortunately, HIT is not a one-size-fits-all situation. The way in which a vendor tests its products may be different from the way in which the products are used in a specific hospital or health system. Some of these differences may be related to how HIT systems are used, the IT infrastructure, and the interfaces to other systems. The following hypothetical example further illustrates this point: let us assume that a 10Gbps infrastructure running a Computer Physician Order Entry application for 15,000 users will perform properly. Under different circumstances, the same application might run poorly.

For example, if deployed over a 1Gbps infrastructure, supporting 15,000 users and 16 interfaces to other administrative and clinical systems, the application could run slowly, crash, or experience a memory leak (which is caused by bug in a computer program that prevents it from freeing up memory that it no longer needs).

Test Lab Environment

A test lab is the best way to ensure effective HIT testing—a lab is like an insurance policy that helps prevent catastrophic outages that may affect hospital revenue, cripple operations, expose the organization to liability, and damage the organization's brand.

Testing an organization's applications, infrastructure, and devices requires an isolated test environment with dedicated technologies and staff. It is important that the lab closely replicate the HIT and conditions within the organization's work environment, and provide a comfortable work space for staff. Placing the lab onsite or near the hospital will enable staff to integrate lab testing into their everyday activities.

The test lab should be sufficient in size to accommodate all network hardware, biomedical devices, and testing tools. Lab staff should include Microsoft and UNIX network applications engineers, and individuals with expertise running tests and writing test cases. Staff should be augmented occasionally with users who want to test specific applications for their user interface; in this way, clinicians can provide feedback prior to the products being purchased or deployed.

Test Lab Costs

The costs to establish a test lab vary depending on the size of the lab, testing tools, and network infrastructure. For example, the estimated cost to set up a lab to test a 250-bed hospital ranges from \$4 million to \$6 million and includes servers, virtualization software, testing tools, and enterprisewide software licenses. Additional costs could be incurred to build out the space needed to store the lab's hardware in a data center, provide room for personnel, and buy additional software licenses. Given this estimate, it is reasonable to assume that build-out costs could reach \$8 million to \$10 million and include approximately 20 percent of initial capital expenses to refresh technology each year. At the same time, initial setup costs should be recovered in three to five years based on the productivity costs affected by system degradation.

Building a Cost-effective Lab

There are a number of ways to save money when building a test lab. One way is an approach called "selected representation and testing tools." With this approach, a duplicate IT environment is created by simulating some IT with specialized testing tools. Tools such as Smartbits simulate user behavior and network traffic. In addition, monitoring tools are used to determine the health of IT during testing. Examples of these tools include the CiscoWorks family of products from Cisco, and Hewlett-Packard's OpenView management software.

Virtualization is another way to save money. Virtualization enables a single, powerful server to replace many individual servers, reducing the lab's computing costs.

Planning and Implementation: Critical Success Factors

While test labs offer many benefits, they do pose some challenges. First, they can be expensive to build. Second, they need executive buy-in from the organization before they can be built. Third, labs must offer a consistent approach to testing. Finally, labs require an ongoing commitment not only to funding, but also to staffing and maintaining an operational strategy. As stated earlier, technology is a business problem, not an IT issue. Strong alignment among the organization's decision makers, business owners (doctors, nurses, and other staff), and IT department is critical to the success of the test lab.

To produce meaningful results, the lab will require both initial funding and upkeep to make sure changes in hardware, software, or biomedical applications are replicated in the laboratory environment. Equipment must also be refreshed constantly as the organization changes technology systems. Lab engineers will require further education on any new technologies under consideration by the organization.

A successful lab ultimately requires cross-organization collaboration.

Developing a Laboratory

Before building a test lab, the following steps are required to ensure that the organization's technology systems meet its needs:

- Assess needs by identifying and mapping the most critical business processes.
- Make sure that the business owners work with the IT department to determine which technology systems support these processes.
- Create an interdisciplinary team to determine how and what should be tested.
- Choose the location for the lab.

Establishing a baseline for the organization's current IT environment is also critical to determining the initial scope and focus of the test lab. It is important to examine the hospital's current and future technology systems to determine how and where IT degradation and downtime might occur. The Cisco Discovery Tool is one of many solutions that can help hospitals better understand the performance of their IT hardware and software systems.

Test Lab: an Essential Capability for Risk Management

An effective HIT environment is critical to the operations of hospitals and health systems. A well-tuned HIT infrastructure maintains a smooth working environment that improves clinician efficiency, promotes patient safety, and helps sustain a positive patient experience. As healthcare organizations continue to adopt new technologies, effective HIT testing will improve the clinical and operational performance of health systems.

A test lab specific to the organization affords comprehensive system testing and validation; eases installation and adoption of technologies; and enables optimal performance and maintenance, even under extreme conditions.

Hospital capital budgets usually address new medical technologies and future investments in clinical applications and devices, along with new facilities and services. The time has come to include an HIT testing program in the capital-budget mix. It is critical that hospitals recognize the importance of HIT testing to all of their health system programs. The test lab is a giant step toward providing excellence in quality care. Making it a part of standard business operations is essential to becoming a leader in the health industry.

Appendix A

This section highlights the major types of vendor IT testing.

Compatibility testing. Ensures compatibility of an application/infrastructure with different hardware, software, or operating systems.

Functional testing. Validates an application/hardware platform for compliance with required features or functions.

Stress and load testing. Evaluates what happens at varying levels of use. Products are tested to determine whether they meet their stated capacity requirements. Products are further tested to determine the load under which they fail and how they fail.

Regression testing. Allows a consistent, repeatable process to validate new releases of hardware or software. Similar to a semiautomated functional test, regression tests are designed to ensure that previous defects have been corrected in subsequent releases, while confirming that no new quality problems are introduced.

Failure mode and effects analysis (FMEA). Analyzes failure modes within an IT system by severity. The effects of component failure on the system are further analyzed.

Appendix B

Testing Approaches and Options

Several approaches are used to test HIT. Each has its merits and limitations. Health system leaders must determine which type of testing method is their best starting point. For any health system at EMR-adoption level 3 or higher, the best option is Selected Representation with Testing Tools.

Individual product testing: This is the most common type of testing method, where software and hardware products are tested in isolation. While this method is an effective way to test individual product performance and functionality, it fails to show compatibility issues with hardware or software, or what happens in an end-to-end customer environment. This means that business risks such as security breaches likely will go undetected.

Selected representation: Selected representation enables an organization to test specific parts of its applications or infrastructure. This type of testing replicates a small subset of the organization's IT and is significantly better than individual testing because it contains a larger IT sample. The downside, however, is that selected representation does not enable testing of the entire production environment, only the replicated components; therefore, it does not produce entirely credible results of how the technology will perform in the production environment.

Full replication: This type of test mirror's a hospital's IT production environment, producing extremely credible results. While technically viable, full replication testing is generally infeasible due to technology and personnel costs because it requires the organization to build a second, complete IT environment.

Shared services test lab: In this type of lab, customers (organizations) rent the space to test a subset of applications or workflows. An example of an application is a nurse using electronic documentation supported by a generic infrastructure that includes routers, switches servers, storage, and telephony. While more cost-effective than building an organization-specific lab, this type of lab does not enable applications to be tested in an environment similar to the actual organization. The absence of a production-like infrastructure limits the credibility of test results. This is especially true with any performance constraints derived from the network, storage, or server hardware.

References

“All Systems Down,” Scott Berinato, *CIO* magazine, 2003,
(<http://www.cio.com.au/index.php/id;1681249874>).

“Calculating the Cost of Healthcare IT Downtime: A New Model for Health Systems,”
Mike Gibbs and Frances Dare, Cisco Internet Business Solutions Group, 2008.

“Stage 6 Hospitals: The Journey and the Accomplishments,” Mike Davis,
HIMSS Analytics, 2007.

“Stage 6 Hospitals: The Journey and the Accomplishments,” Robert Dearborn,
et al, HIMSS Analytics, 2007.

eHealth Vulnerability Reporting Program study, 2007,
(<http://www.net-security.org/secworld.php?id=5466>).

“Security Breaches Cost \$90 to \$305 per Lost Record,” Sharon Gaudin,
Information Week, 2007,
(<http://www.informationweek.com/news/showArticle.jhtml?articleID=199000222>).

“The Cost of HIT Downtime—a New Model for Health Systems,” Mike Gibbs and
Frances Dare, Cisco Internet Business Solutions Group, 2008.

“EMR Sophistication Correlates to Hospital Quality Data,” HIMSS Analytics, 2007.

More Information

The Cisco Internet Business Solutions Group (IBSG), the global strategic consulting arm of Cisco, helps CXOs and public sector leaders transform their organizations—first by designing innovative business processes, and then by integrating advanced technologies into visionary roadmaps that address key CXO concerns.

For further information about IBSG, visit <http://www.cisco.com/go/ibsg>



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.