

REAL WORLD CASE

4

JetBlue and the Veterans Administration: The Critical Importance of IT Processes

When most people think of information technology, software and hardware immediately come to mind. While these are certainly important, good IT processes, particularly those that need to kick in during a disaster situation, are also critical. Most important, these need to be in place before, and not after, they are needed. For example, go back to February 2007, when JetBlue Airways was forced to cancel more than 1,000 flights after an ice storm.

"For one, we didn't have enough of our home-office employees or crew members trained on our reservation system, so while we were dispatching people to the airports to help, which was great, they weren't trained to actually use the computer system. So we're going through a process now where we're actively training those crew members," says spokesman Eric Brinker. The discount airline is also in the process of expanding the capabilities of its reservation crew members so they can accept more inbound calls. "We basically maxed out," Brinker said. "We're working on a system to be able to automatically notify them better to take phone calls."

In the middle of the crisis, JetBlue's IT department developed a database that allowed the airline's scheduling team to improve multitasking. "They were receiving tons of phone calls from our crew members, and we created a database to enter in the whereabouts of our crew members. Then that information would sync up with the information about the crew members that was in the main system," Brinker said. "Now, during a weather situation, our flight crews and flight hands can call us and give us the location of where they are, and we can start to rebuild the airline immediately using this tool. We do that by cross-referencing where the crew members say they are versus where the computer says they are, which weren't always in sync."

Brinker said the airline had never experienced a full meltdown before, so it hadn't needed to use this type of database. "The system, which was developed in 24 hours and implemented in the middle of JetBlue's crisis, has now been implemented as a full-time system," he said. "It's a real behind-the-scenes improvement for both our crew members and customers," he said. JetBlue is also improving the way it communicates with its customers, including pushing out automated flight alerts to customers via e-mail and mobile devices.

Even seemingly smaller and less critical processes can have ramifications of a large magnitude in the interconnected world in which we live. In September 2007, during a hearing by the House Committee on Veterans' Affairs, lawmakers learned about an unscheduled system failure that took down key applications in 17 Veterans Administration (VA) medical facilities for a day. Dr. Ben Davoren, the director of clinical informatics for the San Francisco VA Medical Center, characterized the outage as "the most significant technological threat to patient safety the VA has ever had." Yet the shutdown grew from a simple change in management procedure that wasn't properly followed. The small, undocumented

change ended up bringing down the primary patient applications at 17 VA medical centers in northern California.

The breakdown exposed just how challenging it is to effect substantial change in a complex organization the size of the VA Office of Information & Technology (OI&T). Begun in October 2005 and originally scheduled to be completed by October 2008, the "reforming" of the IT organization at the VA involved several substantial goals. As part of the reform effort, the VA was to shift local control of IT infrastructure operations to regional data-processing centers.

Historically, each of the 150 or so medical centers run by the VA had its own IT service, its own budget authority, and its own staff, as well as independence with regard to how the IT infrastructure evolved. All of the decisions regarding IT were made between a local IT leadership official and the director of that particular medical center. While that made on-site IT staff responsive to local needs, it made standardization across sites nearly impossible in areas such as security, infrastructure administration and maintenance, and disaster recovery.

On the morning of August 31, 2007, staffers in medical centers around northern California starting their workday quickly discovered that they couldn't log onto their patient systems. The primary patient applications, Vista and CPRS, had suddenly become unavailable. Vista, which stands for Veterans Health Information Systems and Technology Architecture, is the VA's system for maintaining electronic health records. CPRS, the Computerized Patient Record System, is a suite of clinical applications that provides an across-the-board view of each veteran's health record. It includes a real-time order-checking system, a notification system to alert clinicians of significant events, and a clinical reminder system. Without access to Vista, doctors, nurses, and others were unable to pull up patient records.

"There was a lot of attention on the signs and symptoms of the problem and very little attention on what is very often the first step you have in triaging an IT incident, which is, 'What was the last thing that got changed in this environment?'" Director Eric Raffin said.

The affected medical facilities immediately implemented their local contingency plans, which consist of three levels: the first of those is a fail-over from the Sacramento Data Center to the Denver Data Center, according to Bryan D. Volpp, associate chief of staff and clinical informatics. Volpp assumed that the data center in Sacramento would move into the first level of backup—switching over to the Denver data center. It didn't happen.

On that day, the Denver site wasn't touched by the outage at all. The 11 sites running in that region maintained their normal operations throughout the day. So why didn't Raffin's team make the decision to fail over to Denver? "What the team in Sacramento wanted to avoid was putting at risk the remaining 11 sites in the Denver environment,

44 • Module I / Foundation Concepts

facilities that were still operating with no glitches. The problem could have been software-related," Raffin says. In that case, the problem may have spread to the VA's Denver facilities, as well. Since the Sacramento group couldn't pinpoint the problem, they made a decision not to fail over.

Greg Schulz, senior analyst at The Storage I/O Group, said the main vulnerability with mirroring is exactly what Raffin feared. "If I corrupt my primary copy, then my mirror is corrupted. If I have a copy in St. Louis and a copy in Chicago and they're replicating in real time, they're both corrupted, they're both deleted." That's why a point-in-time copy is necessary, Schulz continued. "I have everything I need to get back to that known state."

According to Volpp, "the disruption severely interfered with our normal operation, particularly with inpatient and outpatient care and pharmacy." The lack of electronic records prevented residents on their rounds from accessing patient charts to review the prior day's results or add orders. Nurses couldn't hand off from one shift to another through Vista, as they were accustomed. Discharges had to be written out by hand, so patients didn't receive the normal lists of instructions or medications, which were usually produced electronically.

Volpp said that within a couple of hours of the outage, "most users began to record their documentation on paper," including prescriptions, lab orders, consent forms, and vital signs and screenings. Cardiologists couldn't read EKGs, since those were usually reviewed online, nor could they order, update, or respond to consultations.

In Sacramento, the group finally got a handle on what had transpired to cause the outage. "One team asked for a change to be made by the other team, and the other team made the change," said Raffin. It involved a network port configuration, but only a small number of people knew about it. More important, said Raffin, "the appropriate change request wasn't completed." A procedural issue was at the heart of the problem. "We didn't have the documentation we should have had," he said. If that documentation for the port change had existed, Raffin noted, "that would have led us to very quickly provide some event correlation: Look at the clock, look at when the system began to degrade, and then stop and realize what we really needed to do was back those changes out, and the system would have likely restored itself in short order."

According to Evelyn Hubbert, an analyst at Forrester Research Inc., the outage that struck the VA isn't uncommon. "They don't make the front page news because it's embarrassing." Then, when something happens, she says, "it's a complete domino effect. Something goes down, something else goes down. That's unfortunately typical for many organizations." Schulz concurred. "You can have all the best software, all the best hardware, the highest availability, you can have the best people," Schulz said. "However, if you don't follow best practices, you can render all of that useless."

Source: Adapted from Linda Rosencrance, "Overwhelmed IT Systems Partly to Blame for JetBlue Meltdown," *Computerworld*, February 20, 2007; and Dian Schaffhauser, "The VA's Computer Systems Meltdown: What Happened and Why," *Computerworld*, November 20, 2007.

CASE STUDY QUESTIONS

1. Eric Brinker of JetBlue noted that the database developed during the crisis had not been needed before because the company had never experienced a meltdown. What are the risks and benefits associated with this approach to IT planning? Provide some examples of each.
2. With hindsight, we now know that the decision made by Eric Raffin of the VA not to fail over to the Denver site was the correct one. However, it involved failing to follow established backup procedures. With the information he had at the time, what other alternatives could he have considered? Develop at least two of them.
3. A small, undocumented change resulted in the collapse of the VA system, largely because of the high interrelationship between its applications. What is the positive side of this high degree of interconnection, and how does this benefit patients? Provide examples from the case to justify your answer.

REAL WORLD ACTIVITIES

1. Go online and search for reports on the aftermath of these two incidents. What consequences, financial and otherwise, did the two organizations face? What changes, if any, were implemented as a result of these problems? Prepare a report and present your findings to the class.
2. Search the Internet for examples of problems that companies have had with their IT processes. Break into small groups with your classmates to discuss your findings and what solutions you can propose to help organizations avoid the problems you discovered.