FEATURE

The VA's computer systems meltdown: What happened and why

Not following best practices can render the best technology useless

By Dian Schaffhauser

Computerworld |
NOV 20, 2007 12:00 AM PST

At times, the bad news coming from the **U.S. Department of Veterans Affairs** seems unstoppable: D-grade medical facilities, ongoing security and privacy breaches, and a revolving door of departing leadership. In September, during a hearing by the House Committee on Veterans' Affairs, lawmakers learned about an unscheduled system failure that took down key applications in 17 VA medical facilities for a day.

Show notifications

Characterized by Dr. Ben Davoren, the director of clinical informatics for the San Francisco VA Medical Center, as "the most significant technological threat to patient safety the VA has ever had," the outage has moved some observers to call into question the VA's direction in consolidating its IT operations. Yet the shutdown grew from a simple change 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. As a result, the schedule to centralize IT operations across more than 150 medical facilities into four regional data processing centers has been pulled back while VA IT leaders establish what the right approach is for its regionalization efforts.

The Region 1 Field Operations breakdown of Aug. 31 exposed just how challenging effecting substantial change is 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: the creation of major departments along functional areas such as enterprise development, quality and performance, and IT oversight and compliance; the reassignment of 6,000 technical professionals to a more centralized management; and the adoption of 36 management processes defined in the Information Technology Infrastructure Library (ITIL).

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.

The operations of its 150 medical facilities would relocate to four regional data processing centers, two in the east and two in the west. The latter, Regions 1 and 2, are located in Sacramento, Calif., and Denver respectively, run as part of the Enterprise Operations & Infrastructure (OPS) office.

Show notifications

A difficult day

On the morning of Aug. 31, the Friday before Labor Day weekend, the Region 1 data center was packed with people. According to Director Eric Raffin, members of the technical team were at the site with staffers from Hewlett-Packard Co. conducting a review of the center's **HP AlphaServer** system running on Virtual Memory System and testing its performance.

About the same time, staffers in medical centers around Northern California starting their workday quickly discovered that they couldn't log onto their patient systems, according to congressional testimony by Dr. Bryan D. Volpp, the associate chief of staff and clinical informatics at the VA's Northern California Healthcare System. Starting at about 7:30 a.m., the primary patient applications, Vista and CPRS, had suddenly become unavailable.

Vista, **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 provide 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.

At the data center in Sacramento, with numerous technicians as witnesses, systems began degrading with no apparent cause. Instantly, technicians present began to troubleshoot the problem. "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?'" Raffin said.

The affected medical facilities immediately implemented their local contingency plans, which consist of three levels: the first level of backup is a fail-over from the Sacramento Data Center to the Denver Data Center -- handled at the regional level, and the second level of backup is accessing read-only versions of the patient data. The final level of backup is tapping a set of files stored on local PCs at the sites containing brief summaries of a subset of data for patients who are on-site or who have appointments in the next two days, according to Volpp.

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.

According to Raffin, the platform has been structured to perform synchronous replication between the two data centers in Sacramento and Denver. "That data is written simultaneously in both facilities before the information system moves to the next stream or thread that it's processing," Raffin said. "At any instant in time, the same data lives in Sacramento that [lives] in Denver." The systems are built in an autonomous model, he said, so that if something strikes only one facility, the other data center won't be affected.

A failure to fail over

On Aug. 31, 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?

On that morning, as the assembled group began to dig down into the problem, it also reviewed the option of failing over. The primary reason they chose not to, Raffin said, "was because we couldn't put our finger on the cause of the event. If we had been able to say, 'We've had six server nodes crash, and we will be running in an absolutely degraded state for the next two days,' we would have been able to very clearly understand the source of our problem and make an educated guess about failing over. What we faced ... was not that scenario."

What the team in Sacramento wanted to avoid was putting at risk the remaining 11 sites in the Denver environment, 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.

Show notifications

Greg Schulz, senior analyst at **The Storage I/O Group**, said the main vulnerability with mirroring is exactly what Region 1 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." Without it, the data may not be transactionally consistent.

At the affected medical facilities, once the on-site IT teams learned that a fail-over wasn't going to happen, they should have implemented backup stage No. 2: accessing read-only patient data. According to Raffin, that's what happened at 16 of the 17 facilities affected by the outage.

But the process failed at the 17th site because the regional data center staff had made it unavailable earlier in the week in order to create new test accounts, a procedure done every four to six months. From there, medical staff at that location had no choice but to rely on data printed out from hard disks on local PCs.

According to Volpp, these summaries are extracts of the record for patients with scheduled appointments containing recent labs, medication lists, problem lists and notes, along with allergies and a few other elements of the patient record. "The disruption severely interfered with our normal operation, particularly with inpatient and outpatient care and pharmacy," Volpp says.

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 the way they were accustomed to doing it -- through Vista. 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 consultations be ordered, updated or responded to.

Show notifications

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 importantly, said Raffin, "the appropriate change request wasn't completed." At the heart of the problem was a procedural issue. "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 said, "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."

When the Region 1 team realized what needed to happen, it made the decision to shut down the 17 Vista systems running from the Sacramento center and bring them back up one medical facility at a time, scheduled by location -- those nearing the end of their business day came first. Recovery started with medical sites in the Central time zone, then Pacific, Alaska and Hawaii. By 4 p.m., the systems in Northern California facilities were running again.

But, according to Volpp, although Vista was up, the work wasn't over. Laboratory and pharmacy staffers worked late that Friday night to update results and enter new orders and outpatient prescriptions into the database. Administrative staffers worked for two weeks to complete the checkouts for patients seen that day. "This work to recover the integrity of the medical record will continue for many months, since so much information was recorded on paper that day," he says.

Show notifications

A shortage of communication

During the course of the day, said Volpp, affected facilities didn't receive the level of communication they'd been accustomed to under the local jurisdiction model of IT operation. As he testified to Congress, "During prior outages, the local IT staff had always been very forthcoming with information on the progress of the failure and estimated length even in the face of minimal or no knowledge of the cause. To my knowledge, this was absent during the most recent outage."

Raffin denies this. "There were communications," he said. "There most certainly were." But, he acknowledged, they were not consistent or frequent enough, nor did they inform the medical centers sufficiently about implementing their local contingency plan. "It was," he said, "a difficult day."

Once the team realized what it needed to do to bring the systems back to life, Region 1 began providing time estimates to the medical facilities for the restoration of services.

The rift exposes a common problem in IT transformation efforts: Fault lines appear when management reporting shifts from local to regional. According to Forrester's Hubbert, a major risk in consolidating operations is that "even though we're thinking of virtualizing applications and servers, we still haven't done a lot of virtualization of teams." More mature organizations -- she cited high-tech and financial companies -- have learned what responsibilities to shift closer to the user.

Workforce reshaping

Page 1 of 2 ›