the Availability Digest

www.availabilitydigest.com

Sidekick: Your Data is in 'Danger'

November 2009

Sidekick, a popular smart phone provided by Microsoft and marketed by T-Mobile, suffered an outage in early October, 2009, that threatened to wipe out all of the data of its one million worldwide subscribers. Gone were contact lists, photos, calendars, and to-do lists. After initially announcing that all data had been lost, Microsoft then held out hope that some of it could be recovered. The jury is still out on how successful Microsoft will be.

How could this have happened? Especially to Microsoft?

Sidekick and Danger

Sidekick is one of the original smart phones. It is the creation of a company aptly named Danger, started by a team of Apple veterans in January, 2000. Danger called its original smart phone "Hiptop."

Hiptop supported all of the expected smart phone services, including web browsing, instant messaging, games, multimedia, social networking, web e-mail, personal information management, and downloadable software applications. As part of the Hiptop service, Danger set up a server complex - its Service Delivery Engine - to store all of its subscribers' data. This included subscribers' address books, calendars, photos, and to-do lists, as well as email messages.

By doing this, if a subscriber lost his phone, its contents could be easily restored to a new one. Also, if a phone shut down improperly or encountered any corruption of data, Danger could replace the entire data set in the phone with a correct copy.

Microsoft Acquires Sidekick

In early 2008, Microsoft announced its acquisition of Danger and the Hiptop product, apparently in an attempt to shore up its sagging mobile operating system. At the time, Danger had revenues of $56 million and 1.2 million subscribers supported by a staff of 300. Though the purchase price was not announced, speculation is that it lay in the range of $100 million to $500 million.

Microsoft rebranded the Hiptop smart phone as "Sidekick."

T-Mobile and Sidekick

From its earlier days, Hiptop, and now Sidekick, has been marketed by T-Mobile as its smart-phone service. T-Mobile now relies on Microsoft for the backend operations of the Sidekick service.

T-Mobile is a unit of Deutsche-Telekom. With 150 million subscribers worldwide, it is the eighth largest mobile operator in the world and is the fourth largest mobile service in the U.S.

Sidekick

The Sidekick smart phone stores subscriber data in its local RAM. Since the amount of this data can easily exceed the phone's memory capacity, especially with photos, the Sidekick service stores each subscriber's data in its central data center.

Should the phone be turned off and its local data be lost, the phone will resynchronize with the central database when it is next turned on. The Sidekick phones are clients to the central data center's servers and can request not only a database refresh but any piece of data, such as a photo, that the subscriber requests.

Microsoft's central Sidekick server complex is the original Danger system. Microsoft inherited this system and elected not to overhaul it. It is reported to run on Sun Linux servers organized as a cluster with an Oracle RAC database.

Of note is that Sidekick did not provide a means for subscribers to back up their data locally. Subscribers were totally dependent upon being able to retrieve their data from the central servers. In contrast, smart phones such as Apple's iPhone allow subscribers to back up their data to a local PC.

The Data-Loss Disaster

The Outage

On Thursday, October 1, 2009, Sidekick subscribers around the world lost all data functionality. Though the Sidekicks still functioned as mobile phones, all access to address books, calendars, photos, and other data was gone.

Shortly thereafter, users started reporting in a variety of blogs and on Twitter that their Sidekicks were wiped of all personal information. The worst possible outcome was confirmed on Saturday, October 10th, when T-Mobile and Microsoft announced that all data stored for the Sidekick service was likely lost. T-Mobile's statement said in part:

> "Regrettably, based on Microsoft/Danger's latest recovery assessment of their systems, we must now inform you that personal information stored on our device – such as contacts, calendar entries, to-do lists or photos – that is no longer on your Sidekick almost certainly has been lost as a result of a server failure at Microsoft/Danger. That said, our teams continue to work around-the-clock in hopes of discovering some way to recover this information, However, the likelihood of a successful outcome is extremely low."

T-Mobile offered tips to preserve whatever data was still stored in the phones – don't turn them off, don't let the batteries run down, don't remove the batteries. In other words, keep the phone's RAM powered up so that any data that was stored in the phone would remain there until the servers were restored.

On Monday, October 12th, Microsoft chimed in and said in an emailed statement that the recovery process has been "incredibly complex" because the central servers had suffered a confluence of errors from a server failure that hurt its main and backup databases supporting Sidekick users.

This problem wasn't caused by T-Mobile. T-Mobile was let down by its partner, Microsoft. But it was certainly T-Mobile's problem to manage. In response to the magnitude of the outage, T-Mobile suspended sales of both of its current models of Sidekick and offered to allow customers to withdraw from their contracts. It also offered a free month of data service (with a typical value of $20).

This wasn't enough to ward off the inevitable. On October 14th, a class action lawsuit was launched against Microsoft and T-mobile. The lawsuit alleged:

> *"T-Mobile and Microsoft promised to safeguard the most important data their customers possess and then apparently failed to follow even the most basic data protection principles. What they did is unthinkable in this day and age."*

Well said.

The Recovery?

Surprisingly, a few Sidekick users started to report that their personal data, feared lost forever, appeared to be restored. On Thursday, October 15, Microsoft was confident enough to claim that it had recovered most, if not all, of the data and that most Sidekick subscribers would, in fact, see their data recovered

However, a few days later, Microsoft retreated from that position. On Monday, October 19, Microsoft released a sobering statement that said "The Danger/Microsoft team is continuing to work around the clock on the data restoration process. We apologize that this is taking so long, but we want to make sure we are doing everything possible to maintain the integrity of your data. We continue to make steady progress, and we hope to be able to begin restoring personal contacts for affected users this week, with the remainder of the content (photographs, notes, to-do lists, marketplace data, and high scores) shortly thereafter."

On October 20, T-Mobile released a tool on its web site that could be used to recover contacts as of October 1. But Microsoft's hope to restore all data is, as of October 31, still just a hope.

How Did It Happen?

There has not been any statement yet by Microsoft describing the cause of the problem. There has, though, been much speculation in the press about what the problem was. The current speculation is that an upgrade to their storage area network was undertaken without a proper backup, and the upgrade went wrong and wiped out the online primary and backup databases.

Evidently, Hitachi Data Systems was chosen to execute the SAN upgrade. On October 12, T-Mobile stated that ""Hitachi Data Systems is investigating the cause of the problem, which has not been identified at this time."

On October 15, along with its optimistic pronouncement of full data recovery, Microsoft said that a computer system failure caused the loss of data both in a core Sidekick database and in a backup database. It said that it has made changes to improve the Sidekick service's stability and the backup process.

Industry experts have guessed that the problem was not Hitachi's, but rather a Sun cluster/Oracle RAC problem. The Oracle RAC (Real Application Clusters) database allows computers in a cluster to simultaneously access a common database.

As reported in *The Register*,[1] the Danger Service Delivery Engine comprises about twenty CentOS Linux servers and eight or more Sun SPARC and x86 servers running Solaris. Oracle RAC is used as the cluster database for the Sun server cluster.

The outage appeared to be a Sun server failure that was followed by the inability to access user data in the Oracle database and its backup. The Oracle RAC database was fed garbage by the Sun servers and was corrupted during the update process. It seems apparent, though, that the data was not actually deleted; it just couldn't be found until the system was rebuilt and access to it regained

When asked about this conjecture, Microsoft's only response was noncommittal:

> "Sidekick runs on Danger's proprietary service that Microsoft inherited when it acquired Danger in 2008. The Danger service is built on a mix of Danger created technologies and 3rd party technologies. Microsoft's other cloud computing projects are totally separate from the Danger Service and do not rely on the Danger Service technology."

Interestingly, two months previously, Microsoft's Danger subsidiary posted a job ad reading:

> "A key priority is automating reliable reporting log file transfer and database load functionality – existing environment has fragile software and is unreliable, requiring manual DB cleanup and re-run of data loads, retrieving missing files, etc."

Microsoft says that it is rebuilding the Danger Service Delivery Engine piece-by-piece and is recovering more data at each step. This appears to be behind its hope to recover most or all of the lost subscriber data.

Microsoft Has Plenty of Company

This wasn't the first time that Sidekick made the news. In 2005, Paris Hilton's Sidekick was hacked and its contents posted on the Internet.

More to the point, Nokia's Ovi smart phone service suffered a similar outage in February, 2008, when it lost three weeks of subscriber data due to a chiller failure in its data center. In a message posted to its subscribers, Nokia explains:[2]

"A cooler broke down in the hosting center that we run the Chat service in. This event led to two catastrophic consequences from our point of view. Firstly, we had to ramp down the service for a very long period, in fact most of the yesterday morning. Secondly, our database broke down. Despite the fact that we had regular backups, we were not able to set it right. What we had to eventually do was to return to a back-up copy from our previous hosting center, created on the 23rd January 2008. As a consequence, anything you've done since that (profile details, images, friendships) are gone."

Ovi's Apology

[1] Oracle and Sum fingered for Sidekick fiasco**,** *The Register*; Oct. 19, 2009.
[2] Contacts on Ovi beta database failed – my deepest and most sincere apologies, *Nokia Betalabs Blog*; February 12, 2008.

Indeed, other cloud providers have also had news-worthy outages, including Google, Twitter, PayPal, Rackspace, Windows Azure, Salesforce, and Amazon S3.[3]

Lessons Learned

The main lesson to be learned by the Sidekick experience is one that has been voiced over and over in the press, including the *Availability Digest*. If you are going to store your data in the cloud, back it up independently. This best practice extends beyond smart phone data – it must be done for any data you store in the cloud.

Appropriate backup means include your own PC or server, external hard disks, and even another independent cloud.

An interesting and powerful step has been taken in this direction by Amazon and its cloud services. It has established Availability Zones that provide geographically-separated redundancy for its cloud services.[4] A customer can select an Availability Zone to launch an instance of his application. He can also launch a backup instance in another Availability Zone. One of these instances is the primary instance. The database in the backup instance is kept synchronized with the primary data database via data replication.

Perhaps cloud services will someday warrant the trust of your data. Until then, make sure that you keep your own copy.

References

Thanks to Stephen De Dalto, Ron LePedis, and Bruce Holenstein for bringing this story to our attention.

In addition to the references noted above, information for this article was taken from Wikipedia and from the following sources over the period October 1 to October 20:

Wall Street Journal
Computerworld
Network World
Yahoo! Finance
PC World
ZDNet
Reuters
Associated Press
CNet News
The Register
Data Center Knowledge
TechCrunch
ChannelWeb
The ToyBox
Channel Register
Fierce Wireless

[3] The Fragile Cloud, *Availability Digest*; June 2009.
http://www.availabilitydigest.com/public_articles/0406/fragile_cloud.pdf
[4] Can You Trust the Compute Cloud?, *Availability Digest*; August 2008.
http://www.availabilitydigest.com/public_articles/0308/amazon.pdf