

Singapore Bank Downed by IBM Error

August 2010

Déjà vu. Just four months ago, in our April issue, we related Google's experience¹ with incomplete documentation that took down the entire Google Apps data center for two and a half hours. A major Singapore bank, DBS Bank, has just had a repeat of that experience. Only in this case, its systems were down for up to nine hours during a busy banking day. Gone were its online banking, its ATMs and credit-card services, and its back office systems.

The problem was caused by an IBM employee who directed operations staff to use an outdated procedure to perform maintenance on a disk-storage system. The correct procedure had yet to be documented.

The bank compounded the problem by waiting too long to dust off its business continuity plan. By the time the bank convened its disaster recovery team, the crisis was almost over.

DBS Bank

DBS Bank is the largest bank in Southeast Asia and a leading bank in Singapore and Hong Kong. With four million customers, 1.4 million of which do online banking, DBS manages almost 1,000 ATMs and 100 branches in Singapore and Hong Kong and has operations in 15 markets, including China, Taiwan, India, Thailand, Malaysia, the Philippines, and Indonesia.



The bank began operations in 1968 as a development financing institution led by the Singapore government. It was known as the Development Bank of Singapore until it changed its name to DBS Bank in 2003 to reflect its growing role as a major regional bank in Southeast Asia.

The Outsourcing Decision

In 2002, DBS contracted with IBM to run much of its data-center services. The outsourcing contract was set for ten years at a cost of S\$1.2 billion (a Singapore dollar was worth about 0.73 U.S. dollars at the time). As part of the outsourcing arrangement, 500 DBS Bank staff were transferred to IBM. IBM built new data-center facilities in Singapore and Hong Kong to house the DBS IT systems.

¹ [Poor Documentation Snags Google](http://www.availabilitydigest.com/public_articles/0504/google_power_out.pdf), *Availability Digest*, April 2010.

An important element of IBM support is the IBM Asia-Pacific team. Among other capabilities, this team is the central support for all IBM storage systems in the Asia-Pacific region, whether they are inhouse or outsourced. This team was to play a major role leading to the DBS outage.

The Outage

Early Warning

The timeline for this outage began about forty hours before the actual outage occurred. On Saturday morning, July 3rd, IBM operations staff in the Singapore data center began to receive alert messages. The messages indicated instability in a communications link within a major storage system used by most of the bank's mainframe applications. However, the bank's systems are highly redundant and are designed for high resiliency. Consequently, the storage system was still fully functional.

Therefore, the problem was classified as "low severity," and corrective maintenance was scheduled for 3 AM, Monday, July 5th, a quiet time for the bank.

The Maintenance Fiasco

A summary timeline compiled by *BusinessTimes.com.sg*, which cited DBS and IBM as its sources, showed the following sequence of events.²

"July 3, 11:06 a.m.: IBM software-monitoring tools sent an alert message to IBM's Asia-Pacific support centre outside Singapore, signaling an instability in a communications link in the storage system connected to DBS's mainframe computer. An IBM field engineer was dispatched to the DBS data centre.

"July 3, 7:50 p.m.: The engineer replaced a cable, not using the maintenance instructions on the machine but those given to him by the support-centre staff. Although this was done using an incorrect step, the error message ceased.

"July 4, 2:55 p.m.: The error message reappeared, this time indicating instability in the cable and associated electronic cards. The IBM engineer was dispatched again to the data centre. He asked the regional IBM support centre for advice.

"July 4, 5:16 p.m.: Following instructions from the support-centre staff, the engineer removed the cable for inspection and put it back using the same incorrect step. The error message ceased.

"July 4, 6:14 p.m.: The error message reappeared. Over the next 5 hours and 22 minutes, the regional IBM support centre analysed the log from the machine and recommended to the engineer that he unplug the cable and look for a bent pin. Throughout all this, the storage system was still functioning.

"July 4, 11:38 p.m.: The engineer did not find a bent pin and put the cable back. The error message persisted. The regional support centre and the engineer continued trying to uncover the problem, including unplugging the cable and putting it back again. DBS was contacted and authorised a cable change at 2:50 a.m., a quiet period. While waiting to replace the cable, the IBM engineer decided to inspect the cable again for defects and to check that it was installed properly. He unplugged the cable, again using the incorrect procedure advised by the regional support-centre staff.

² Bob Evans, *Global CIO: IBM's Bank Outage: Anatomy Of A Disaster*, *Information Week*, August 5, 2010.

"July 5, 2:58 a.m.: He replaced the cable using the same procedures as before. This caused errors that threatened data integrity. As a result, the storage system automatically stopped communicating with the mainframe computer in order to protect the data. At this point, DBS banking services were disrupted."

As reported, though this was a routine repair, the IBM repair crew in Singapore sought advice from the regional Asia-Pacific team on how to fix what they thought to be a minor fault in the storage system. A member of that team suggested a procedure that had been regularly used before. Unfortunately, the procedure had been modified and evidently had not been documented. The procedure caused the storage system to crash.

For some reason, the procedure also caused the backup systems to fail. There has been no comment from either the bank or IBM as to why this happened. Suffice it to say that most of the bank's services were now down. Online banking was dead. ATMs were silent. Credit cards could not be used. Commercial banking was halted.



At 3:40 a.m. on July 5th, IBM mobilized the "technical command function," a crisis support team. At 5:20 AM, a restart of the system was attempted; but it didn't work. The crisis was escalated, and the bank-wide "disaster recovery command center" was activated. However, by 8:30 AM, it appeared that the system was close to restoration and that the command center was not needed.

The ATM machines and credit-card operations were restored by 10 a.m., seven hours after the outage. It was another two hours before online banking services were restored at noontime.

Branches opened as usual at 8:30 a.m., but their consoles were dead. The bank authorized the cashing of checks for up to S\$500, and customers could make cash withdrawals over the counter. The branches stayed open an extra two hours that evening to clear up backlogs.

The bank reported that, fortunately, no data was lost and that all transactions that day would complete by end of day.

Management's Response

IBM took full responsibility for the outage. It said that "the failure to apply the correct procedure to fix a simple problem in the data-storage system it maintains for DBS had crashed most of the bank's systems." It committed to improve the training of its support personnel.

It is unusual in Singapore for a CEO to make a public apology. However, Piyush Gupta, DBS' CEO, issued a three-page detailed apology to the bank's customers. He stated that "a procedural error triggered a malfunction in the multiple layers of systems redundancies, which led to the outage."

Gupta also acknowledged that the bank should have escalated the problem earlier and that it could have done more to mobilize broadcast channels to inform customers of the interruption in services the first thing in the morning.

He did confirm, however, that no data was lost as the result of the outage and that all payments and transactions of the day



Piyush Gupta, DBS CEO
Photo: Arthur Lee/BT

had been properly processed.

The Regulatory Response

The Monetary Authority of Singapore (MAS) is Singapore's central bank and financial regulator. Among its many responsibilities is to write regulatory requirements for banking-system outages. In its *Internet Banking and Technology Risk Management Guidelines*, MAS states that users expect online banking services to be accessible "24 hours every day of the year." This is "tantamount to near-zero downtime." MAS guidelines further state that "a bank's responsibilities and accountabilities are not diminished or relieved by outsourcing its operations to third parties or joint-venture partners."

DBS Bank certainly fell short of the reliability benchmarks laid out by MAS. In a statement issued after the outage, MAS said that it would "assess the extent to which the bank has failed to meet the recommended standards set out in the *Internet Banking and Technology Risk Management Guidelines* before determining the appropriate regulatory action to take."

Subsequently, on August 4th, MAS censured DBS for "shortcomings and inadequate management oversight by the bank of its outsourced IT systems." It ordered DBS to redesign its online and branch-banking platforms in order to reduce concentration risk and to allow greater flexibility and resiliency in its operation and recovery capabilities. It also required the bank to improve its customer-communications procedures.

MAS also directed the bank to set aside S\$230 million additional regulatory capital for operational risk.

On IBM's part, it said that it has disciplined the personnel that were directly involved with the outage and removed them from direct customer-support activity. IBM also has appointed technical advisors to provide deeper technical expertise to DBS.

Lessons Learned

As we learned from the Google power-outage disaster that we covered this last April, all procedure changes must be well-documented and tested and the appropriate personnel trained. These activities should all be part of change management. In response to this incident, IBM has stated that it has taken steps to enhance the training of its personnel.

It is also important to know when to escalate a problem to more senior technical staff and to those responsible for public communications and relations. This is an important part of the Business Continuity Plan and should be memorized by all affected personnel. The middle of a crisis is not the time to be confused as to which steps to take.

As is the case in so many outages, communication with DBS users concerning the nature of the outage and the outlook for a return to service was nonexistent. Users can be patient when they know what is going on but brutal if left in the dark.

And yes, outages can have a regulatory impact on the enterprise.

As with most enterprises, this is not the first outage experienced by DBS, though it is the most significant. In September, 2000, all branch services and its ATM network were down for an hour. In September, 2009, a branch problem limited customers to withdrawals under S\$2,000 and prevented them from updating their passbooks. In October, 2009, online banking was down for

three hours. It is important that we learn from each outage and spread the lessons learned among our peers throughout the IT industry.³

Acknowledgements

Our thanks to our Availability Digest subscribers Corinna Tseng and Keith Parris for bringing this incident to our attention. Information for this review was taken from the following articles:

IBM employee sparks massive bank outage, *The Register*; July 13, 2010.
Singapore Bank Suffers Massive IT Outage, *PC World*; July 6, 2010.
Downtime nightmare could cost DBS dearly, *Business Times*; July 7, 2010.
Outsourcing prematurely blamed for DBS outage?, *Business Times*; July 8, 2010.
IBM storage glitch causes massive bank system failure, *Techworld*; July 1, 2010.
Bad advice from support unit caused DBS systems crash, *Business Times*; July 15, 2010.
DBS points outage finger at IBM, *ZDNet Asia*; July 1, 2010.
DBS could have coped better, says CEO, *Business Asia One*; July 1, 2010.
Botched repair caused crash, *Straits Times*; July 14, 2010.
Outdated repair procedure caused DBS system breakdown, *Business Asia One*; July 14, 2010.
DBS Group CEO apologises, *Today Online*; July 14, 2010.
DBS blames IBM, braces for backlash from MAS, *Business Times*; July 14, 2010.
'Give public full account', *Straits Times*; July 13, 2010.
'We have failed you.' *Straits Times*; July 13, 2010.
MAS assessing the extent of DBS' failure, *Business Times*; July 13, 2010.
Singapore Censures DBS, *The Wall Street Journal*; August 4, 2010.
DBS CEO acknowledges censure by MAS, apologises for outage, *Singapore News*; August 4, 2010.
Global CIO: IBM's Bank Outage: Anatomy Of A Disaster, *Information Week*; August 5, 2010.
Singapore central bank slams DBS and IBM over systems outage, *Finextra*; August 5, 2010.

³ More to the point, if you have a story to share that will help others, even if it must be published anonymously, let us know so that we can publish it as a *Never Again* article for the benefit of all.