the Availability Digest

www.availabilitydigest.com
@availabilitydig

Airlines’ Aging IT Technology Is Taking Its Toll

October 2016

First it was Southwest Airlines. In July, 2016, a router failure grounded Southwest for four days.[1] A backup router failed to take over. Though the problem was fixed in twelve hours, the failure wreaked havoc on Southwest’s operations for the next several days as the airline struggled to get planes and crews where they were supposed to be. Over a three-day period, Southwest cancelled 2,300 flights – about 11% of its schedule. Thousands of other flights were delayed.

Next was Delta Air Lines. In August, 2016, a fire in Delta’s data center took down all of its computer operations, causing it to cancel 2,100 flights over three days.[2] Hundreds of other flights were delayed. Delta estimates that the outage cost it $150 million USD in lost revenue and passenger compensation.

Then came British Airways. In September, 2016, a power outage at its hub near Heathrow airport caused a worldwide computer failure. Eleven flights were cancelled, and further BA flights throughout the day experienced two-hour delays.

A United fault last summer lasted for two hours and disrupted travel for thousands of fliers. The outage was caused by a malfunctioning router that prevented the carrier from ticketing passengers and dispatching crews.

JetBlue experienced flight delays last January due to the loss of power at its data center. American Airlines suffered from connectivity issues in September, 2015, and had to suspend flights at Miami, Chicago O’Hare, and Dallas/Fort Worth airports.

The Delta outage shows how a single IT failure at the wrong place and the wrong time can cost an airline millions of dollars. The Delta debacle is a wake-up call for an airline industry in which outdated information systems can strand thousands of passengers and cost an airline millions of dollars.

In 2015, the company Quartz (http://qz.com/) began tracking technical glitches plaguing airlines. It found twenty-four significant airline system failures during this time.

An Aging and Complex Infrastructure

What is happening to the airline’s IT infrastructure? The short answer is that the airlines have to deal with an aging and complex legacy infrastructure.

The systems that many airlines depend upon were first developed decades ago when flights were fewer and passenger options were simpler. For instance, Delta’s passenger check-in system is based on

[1] Southwest Airlines’ Router Grounds 2,300 Flights, *Availability Digest*; August 2016. http://www.availabilitydigest.com/public_articles/1108/southwest_airlines.pdf

[2] Delta Airlines Cancels 2,100 Flights Due to Power Outage, *Availability Digest*; September 2016. http://www.availabilitydigest.com/public_articles/1109/delta.pdf

Deltamatics, a legacy system put into service 52 years ago. The core design of these systems comes from an era when the presumption was the systems would go down every night, creating a maintenance window during which systems could be upgraded.

However, as airlines merged, new features were added to gain competitiveness (for instance, an extra leg-room option in Economy class). These features were added to the original legacy systems, a process made more difficult by the fact that the systems no longer could be brought down for upgrades. Airlines today operate on a 24/7 basis, and their systems must do the same. As function upon function were added to the original legacy systems, the systems became so complex that one small problem could snowball easily into larger ones.

Consequently, complexity, not age, is the real problem. There are so many systems layered on top of each other. Examples of such systems include:

- Reservations
- Passenger check-in
- Aircraft assignment
- Flight crew scheduling
- Airport gate assignment
- Air traffic flow management

Many of these systems have to interact with other systems such as mobile apps, loyalty awards, and the sale of perks like extra leg room.

Improvements are now multi-year and multi-million dollar investments. Every little piece has to work perfectly or the system falls apart.

Is Management to Blame?

What responsibility for these failures should management bear? In Delta's case, the company invested hundreds of millions of dollars in technology upgrades over the last three years to prevent exactly what happened. This included bringing in two independent power sources into its Atlanta data center. However, 300 of Delta's 7,000 servers in the data center did not have dual power supplies, or if they did, the independent power supplies were not plugged into opposite power sources. When one of the power sources failed due to a fire, many of the servers were taken down along with their backups, taking down the entire Delta system.

This is an example of a problem caused by a lack of rigorous management oversight.

Companies with complex IT systems employ safeguards against failure with multiple layers of backup components. When such systems fail, it is much more that a single failed component or a human mistake. It is a failure of management.

In the cases of Southwest and Delta, pilots and the mechanics union blame the outage on cost-cutting.

Management needs to have the transparency and accountability in the reporting chain to ensure processes and management structures are in place and followed in order to prevent or mitigate against these issues. Delta had invested in multiple power paths for its data center. It had everything in place to sustain customer service. However, a lack of processes or enforcement of processes defeated the investment.

The responsibility for cascading failure flows from the top down in an organization. Management can contribute to these failures in many ways:

- Through inadequate staffing and training.

- By encouraging an organizational culture that becomes dominated by a reactive mentality rather than by a proactive approach to predicting and preventing problems.
- Through budget cutting that reduces preventive and proactive maintenance.

IT organizations need to ensure that their people are adequately trained and resourced. They need to ensure procedures are documented and followed and that critical assets are maintained and tested

Even Congress is getting involved. Democratic senators Edward Markey and Richard Blumenthal have sent a letter to thirteen airlines with ten questions regarding recent disruptions, the state of airlines' technology systems, and how airlines accommodate passengers during outages.

Summary

Delta's control points are centralized. The airline runs route scheduling, ticketing, and check-in over a single network. This approach is cost effective, but it runs smoothly only while the central control points are available. A single failure can take the entire network down.

As we've said many times in our articles, not only must you have geographically separated redundancies built into your systems (neither Delta not Southwest did), but failover to redundant components must be periodically tested to ensure that they work.

Both Southwest and Delta had failover faults. Southwest's backup router did not take over when the primary router failed. Many of Delta's servers could not fail over to their backups because they too lost power. Clearly, neither Southwest nor Delta thoroughly tested their failover capabilities.

Acknowledgements

Information for this article was taken from the following sources:

What CIOs can learn from the Delta outage, *CIO Dive*; August 9, 2016.
Airlines at risk from aging technology, *USA Today*; August 12, 2016.
We're learning the wrong lesson from airline IT outages, *Network World*; August 20, 2016
This summer's outages at Delta and Southwest have much to teach all of us in IT, *Network World*; August 31, 2016.
Computer failure hits BA flights, *Daily Mail*; September 18, 2016.
Delta System Failure Marks Wake-Up Call for Airline Industry, *Datacenter Knowledge*; undated.