

REPORT GILLIAN JENNER LONDON

Avoiding an IT meltdown

The impact of recent technology failures at British Airways, Delta and Southwest reflects an industry grappling with reliance on increasingly complex – and critical – systems

When British Airways was forced to ground 726 flights over three days in May, the resulting chaos for its passengers around the globe racked up a bill in the order of £80 million (\$105 million), according to the airline's own estimates. BA found itself under intense scrutiny from the media, and UK Prime Minister Theresa May weighed in, calling on the airline to compensate disgruntled customers.

Less than 12 months earlier, in July 2016, Southwest had axed more than 2,000 flights, thereby slicing \$47 million from its passenger revenues in the third quarter. And across four days in August 2016, Delta cancelled a similar number of flights, clipping an estimated \$150 million from its pre-tax quarterly earnings.

In each case the trigger for these high-profile operational meltdowns was an IT crash. These setbacks are not isolated incidents and, to be fair, not the exclusive preserve of airlines. *Failures in Airline Systems*, a white paper issued last year by Travel Technology Research (T2RL), noted more than 20 newsworthy systems failures between 2010 and 2015 that affected industries such as banking, technology providers, web and email services, as well as aviation.

It is always difficult to establish the detail of a systems failure because businesses understandably do not want to expose their own weaknesses. Whatever the initial cause, be it a power outage, cable cut, router failure or a breakdown in one of the backbone computer systems, these events can rapidly



BA's outage in May affected a range of critical systems

RStevenson/Twitter

escalate to have a significant impact on an airline's customers, staff and business.

While it has become a familiar refrain to bemoan the shortcomings of centralised legacy systems that continue at the heart of more than a few airlines, they remain a key vulnerability. These older bespoke stand-alone systems do not easily lend themselves to working in a cloud environment or using synchronised and remote distributed data centres – more recent technologies with the advantage of built-in redundancy.

"I do think the issues we have seen at some of the major carriers are effectively the canary in the coal mine warning us that some of the antiquated technologies in use at the airlines are somewhat risky when it comes to this area," warns Ron Peri, chairman and founder of Radixx International, a passenger service system provider.

LINEAR DEPENDENCIES

There are other issues in play that can increase any airline's vulnerability to an IT crash. Innate complexity is one of the most likely factors in any serious outage scenario. A daisy chain of systems with linear dependencies effectively ensures system-wide failure sooner or later.

T2RL's chief strategy and research officer, Bert Craven, observes that airline systems are "inherently complex and becoming more complex"; in other words, the more moving parts you have, the more likely a system will fail. He says: "Complexity makes failure scenarios harder to predict, anticipate, plan for and test. It also makes failures harder to diagnose and fix."

Airline systems and the services they provide are consumed globally. "Although 'the system' may be reliable, there is an awful lot of infrastructure between 'the system' and its users," explains Craven, adding that "interconnecting networks from multiple providers, airport common-use terminal equipment (CUTE) and common-use service system (CUSS) platforms, and a variety of other infrastructure, all form part of the end-to-end service".

"I think our industry could afford more redundancy by sharing infrastructure" **Sebastien Fabre, vp Airport Solutions, SITA**

Then consider the backdrop of an air transport sector that relies heavily on technology.

"Technology and automation have allowed processes in airports to operate at a speed and density that has brought many benefits in terms of efficient use of constrained resources," says

Craven. "However, this also means that in many cases there is no longer a practical, manual alternative to fall back on when the technology fails."

A change somewhere on the airline system, for example adding an extra feature or making an upgrade, also makes it more vulnerable to failure. Peri at Radixx cautions: "The more monolithic a system, the greater the risk with the change, because a change means you are changing a very substantial portion of the system.... Areas that worked before might now be broken."

He adds: "There are some companies in the industry – not Radixx, by the way – who suspend their service level agreement [SLA] for 48 hours or more after a change. In other words, their presumption is, we are making a change, there are going to be some problems and that's a risk we are telling you about in advance."

Airlines also need to be aware of the risks when they integrate services from different providers, each with its own SLA. Aside from creating complexity – and the risk of unpredictable failure – airlines could be decreasing their protection. T2RL's white paper notes: "An end-to-end service with a 99.95% monthly SLA can be down for 21 minutes in a month before the provider is in breach. The same service covered by two separate 99.95% monthly SLAs can be down for 42min in a month before any provider is in breach. Add a third and you are over an hour already."

Knowledge gaps in the business, whether as a result of natural churn of experienced IT personnel or through outsourcing IT functions to an external provider, can potentially contribute to the mayhem around an IT outage, particularly if the airline relies on legacy infrastructure. However, there are business tools to capture and manage knowledge.



CNBC

The real issue is experience. "Knowledge can be managed and transferred fairly easily and it exists independently of people," says T2RL's Craven. "Judgement can only come from experience and is almost impossible to transfer from one individual to another." He adds: "Knowledge of technology is not enough; partners must also understand the business".

SITA's vice-president of Airport Solutions, Sebastien Fabre, agrees that a strong knowledge of the business systems plays a vital role in recovery and re-starts, citing a major outage at a large European airport. "The fact that we knew how the systems worked and the ones that needed to be restarted first allowed us to resume as quickly as possible and even actually guide the other service providers in the airport about what to do."

Anish Kapoor, vice-president and head of the Travel Centre of Excellence for Intelnet Global Services, a major business process outsourcer, notes that outsourcers are beginning to hire people with in-depth industry knowledge to align digital solutions that can address some of the challenges airlines face. He adds that outsourcers provide digital expertise to airline staff, helping them to ensure people on the ground are able to respond promptly to customer requests.

"By implementing a more collaborative business model, airlines are better able to prevent knowledge gaps, enabling them to feel empowered and better able to use next generation technologies to be able to cater to customer requests," Kapoor says.

PROACTIVE THINKING

Regardless of whether they are working off a legacy backbone or sitting on a next-generation cloud-based system, airline leadership cannot afford to be complacent about including strategies to combat IT outages both within the technology environment and as part of overall business continuity planning.

Building in resiliency – the ability to provide an acceptable level of fault tolerance despite challenges to normal operations – and redundancy, or back-ups, into an airline's technology ecosystem is the first obvious and vital counter-measure. "As with quality, where everybody has to be thinking quality at all times, it is not something that can be tacked on at the end. Likewise with redundancy," says Peri at Radixx. "It should just be a natural way of thinking for everybody who is involved in the airline and the PSS."

Resiliency and redundancy may be sensible, but they come at a price, which can be a delicate balance to get right. "If you have too much redundancy and too many back-up systems, the cost becomes unaffordable and it impacts ticket price and everything," says Fabre at SITA.

Although he believes the industry has managed to get the balance between risk and redundancy about right, he sees an opportunity to make it more cost-effective. "I think our industry could afford more redundancy by sharing infrastructure....



Typically when we provide infrastructure at airports we are actually sharing it among several airlines. And by sharing infrastructure, we can actually afford more resiliency, more redundancy."

Fabre explains that shared infrastructure in the back end could be anything from telecommunications to software and systems such as bag sortation. He adds that more standards, in terms of best practice and guidelines, are needed to enable sharing as much infrastructure as possible to lower the cost. "If everyone does his own thing, very proprietary, very specifically, it is much more difficult to share infrastructure [and] also understand where you put resiliency, where you put redundancy," he says.

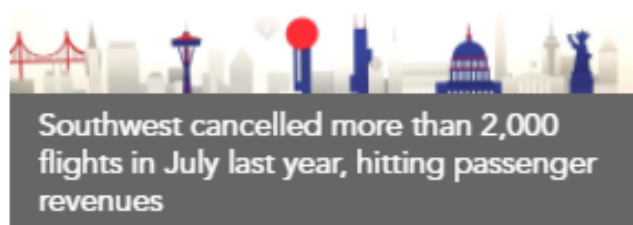
Cloud services also provide redundancy and will be one of the top IT investment priorities over the next three years, with 95% of airlines and 85% of airports planning programmes, according to SITA's recent 2017 Air Transport IT Trends Insights report.

Peri at Radixx sees an opportunity to use the cloud for more than data back-ups. "I would recommend any airline to look at the possibility of their system being backed up in the cloud, not just with data – essentially an operating system in the cloud that is redundant. That is the logical place today to have pure redundancy," he says. "For the legacy systems that's very difficult. For the more modern systems it's much easier. So our entire system can run in the cloud. It's not always the most cost-effective way to do things on a day-to-day basis, but in an emergency, it's a very good solution."

Monitoring tools, which are becoming increasingly sophisticated, can also be deployed to detect warning signs and tackle potential problems before the system collapses. Over the next three years, 80% of airlines and 58% of airports have prioritised investment in technologies that monitor and manage the performance and availability of software applications, according to SITA's IT trends report. Fabre says that from SITA's experience managing airport infrastructure, "75% of the incidents are detected and managed before we receive a call from a customer, meaning before it has a business impact".

Central to successfully bouncing back from an IT outage is planning across the business.

Exception-management scenarios, which encapsulate the expert knowledge of the organisation,



Southwest Airlines

When an airline, or any other business for that matter, keels over and its entire operation stops working, one might surmise that it has failed either to implement or to follow a planned exception-management scenario. Of course, there are always the "unknown unknowns" that cannot be planned for, and it is for this reason there is a movement towards non-linear de-centralised systems that can work around unknown issues.

"In terms of mitigating the impact of the outage, the most significant thing really is if you can shorten the length of time that you have the outage," says Peri. "Key in that is a clear escalation process that is followed."

He observes that typically the engineers trying to diagnose and solve the problem can be within five minutes of the solution for hours, so you need someone who is not lost in the problem to enforce the escalation process. "Who gets called in that escalation is also key. What steps get taken," he says. "If it's planned out, you will have a much better result. If it's ad hoc, then you are dependent upon the quality and knowledge of the individuals who are trying to solve the problem."

For Craven at T2RL, the advance planning should include designing "graceful failure" modes that create a minimum viable operating platform; devising alternative operating procedures, staff policies and guidelines for use during disruptions; and cross-training staff in different roles so that they can fill in during crises.

There may be opportunities to use alternative systems at large hubs, where ground handlers could have their own departure control system (DCS). "An airline could work out a deal with their ground handler that allows them to fail over to the ground handler's DCS in the event that their



RStevenson/Twitter

own main DCS fails," Craven suggests.

"Airlines should be examining and benchmarking their recovery and re-accommodation capabilities against the market to see how and where they might be improved," he adds.

"Response planning, especially communications, to a set of failure scenarios can improve the quality of and accelerate an airline's response in the event of a disruption or crisis."

BEING READY

SITA envisages an opportunity to incorporate IT outages into the business planning for other types of disruption, such as a fire or delayed flights, so that it is part of every department's preparation and training, throughout airlines and airports. "Nobody can really be blamed for being impacted by an outage, especially if it is a power outage or a major cybersecurity attack, but I think we can be blamed as a company if we don't have a procedure ready and we don't have documented action on how to deal with the outage," says Fabre. "Make sure you are ready to do that."

Clearly the current technology investment focus is to move away from monolithic and linear systems. It is worth noting that the logical end point of this de-centralisation is to eliminate a centralised business model as far as possible. Instead, each business node, such as an aircraft or any other major asset, would be self-determining and able to work as a node in a peer-to-peer system. This would allow for much greater fault tolerance and make it easier and cheaper to redefine and change any element of the business.

Reassuring your customers is wise, but rushing in front of camera might not be

Communicating with your staff and customers across multiple media platforms while fire-fighting to get systems back online is stressful. You may even, like BA did earlier this year, find your communications system has gone down alongside the wider IT network. Therefore, like BA chief executive Alex Cruz, it may be necessary to take to YouTube and Twitter to keep people informed.

The secret to keeping everyone on side is clear messaging, timely updates and managing expectations, according to Al Berman, former president and chief executive of the Disaster Recovery Institute International (DRI) and current president of the DRI Foundation.

He recommends avoiding speculation: tell people what you know, and do not use any technical terms as they will think you are hiding behind them. "You are starting to see [airline] talk in more plain language... [and] one of the things that airlines are doing better, they are managing expectations. They are starting to communicate.

"A piece of advice that I give to all CEOs [is] never be the first one in front of the camera, because you are going to say something stupid.... The CEO should just sit back and let someone else make the mistakes. Then



British Airways/Twitter

they can come in and say, 'we have got more facts'," says Berman.

He observes: "You truly cannot rush restoring a system. It takes as much time to try the fix, reboot the system, align your data and all the processes and the quality control that has to take place. But you can manage the expectation. And if you live to that schedule, people think you have done a wonderful job."