451 Research®

# 2016 datacenter failures highlight growing complexity, high-profile consequences

ANDY LAWRENCE

10 OCTOBER 2016

Datacenter failures are not new – sooner or later, almost every site goes down. But failures in 2016 have had high-profile and expensive consequences. Power chain problems, inter-dependencies and IT recoverability are common themes.



VOLTA
Central London's Data Centre

Datacenter failures are not new – in fact, per hour of aggregated uptime, they are far less common than they use to be. But increased dependency on IT, and increased co-dependency between IT systems, means the impact of failures reverberates ever more widely. 2016 has seen some high-profile datacenter incidents that made national news, and, moreover, have proven highly expensive for the operators. Of these, the downtime suffered at Delta and then Southwest Airlines are the most notable.

Unlike in 2014 and 2015 – when security breaches caused the biggest problems (at Sony and UK telecom provider Talk-Talk, for example), there are some common themes in the most recent failures. Failures in the power-distribution equipment have been the root cause of several incidents, and problems with IT recovery have often amplified the severity of the issue. In this report, we list some key failures, identify some of the causes, and consider the implications.

## THE 451 TAKE

In a report earlier this year, we wrote: "the risks and costs of (datacenter) failures are so high that most businesses opt for a very high level of resiliency with little cost-benefit analysis." Is it worth it? we asked – noting that research into the cost and causes of downtime at the datacenter level is thin on the ground (although the evidence suggests the costs of failure are high and rising). There is, however, nothing like a cautionary tale to goad management into making extra efforts and investments – and there are a lot of such examples coming to light. In the coming years, the way that resiliency is achieved at the datacenter and application level is expected to change significantly as we move to a more cloudy, hybrid and distributed environment. In the meantime, the evidence of these incidents suggests that managers need to maintain if not increase their vigilance, because the interdependencies of real-time systems means the costs of failures are higher than ever.

The table below lists a series of failures that occurred from June to the end of September 2016.

| COMPANY/ DATACENTER(S) | DATE(S) | AFFECTED AREAS/EXTENT | CAUSE | COST? |
|---|---|---|---|---|
| Delta Airlines | 8-Aug | All operational systems in NA. | Power surge, power/ transfer switching failure; IT systems corrupted. Some servers didn't have dual power chords? | 1800 flights cancelled. Quarterly earnings expected down 10%. |
| Southwest Airlines | 20-Jul | All operational systems in NA. 12 hour outage, cancellations for several days. | Malfunctioning router triggered multiple problems (IT level). | 2,300 flights cancelled. |
| TeleCity LD8 (Equinix) | 19-Jul | Some Linx traffic. BT Broadand. | UPS failure | Not known/undisclosed |
| Telehouse | 21-Jul | UK and beyond. BT Broadband/email services in UK. 7-10 hours. | "Tripped circuit breaker". | Not known/undisclosed |
| FCA @ Fujitsu Sunnyvale CA | 24-27 Sep | System for managing 50,000 FCAs. | Transformer failure? | 50K financial institutions unable to access. Strategically embarrassing. |
| ING Bucharest | 10-Sep | Banking systems. | Noise from fire suppression systems damages dozens of disk drives. | Systems down for 10 hours. Many storage systems and servers replaced. |

| COMPANY/ DATACENTER(S) | DATE(S) | AFFECTED AREAS/EXTENT | CAUSE | COST? |
|---|---|---|---|---|
| SSP at Solihull datacenter. | 26-Aug – 24-Sep (?) | All core systems. | Power outage at Solihull triggered SAN problems. Second SAN failure followed. Attempting emergency migration to Tier 3. | 40% of UK insurance brokers unable to access renewals data. |
| Global Switch 2, London | 10-Sep | Many customers affected, notably Claranet. | 222ms high voltage drop/ circuit breaker/DRUPS caused 222ms break, triggering shutdowns. Claimed Tier 3 stan-dards... | Not known/undisclosed |
| Global Switch 2, London | 6-Jun | Many customers affected. | Lightning strike led to several hours outage for some customers. | Not known/undisclosed |

## LESSONS AND IMPLICATIONS

The stories of many of these incidents will be told for years to come. Some of these failures will likely have career-changing impacts. Certainly, there were calls for the CEOs of Delta and Southwest Airlines to resign, given the financial cost (at the time of writing, the impact of Delta's downtime has been estimated at $120m).

Although far from the largest, the problems at SSP were so serious and long-lasting that management brought forward parts of a planned migration to a new datacenter. Every situation is different, but there are some insights that can be drawn by looking at these failures together:

- A common lesson taught by engineers and consultants from the Uptime Institute (a sister company of 451 Research focused on datacenter design and management) is that datacenter failures are almost never caused by one problem. This is highlighted by many of these failures. For example, at Delta, a glitch in the power supply was further exacerbated because some servers were not plugged into both the A and B sides of the power chain – demonstrating poor oversight and/or risk taking. This was then further complicated because recovery systems did not properly manage the re-introduction of services, so that databases became corrupted or untrusted.
- Unforeseen problems will occur. No amount of planning can prevent datacenter downtime. ING, for example, suffered an unlikely loss caused by a noise from the fire-suppression system. Although even this had been foreseen, changes in storage technology had rendered some new models more vulnerable.
- Vigilance and investment are essential. Most of the datacenters involved acceptable levels of resiliency – but often, some processes or small design elements had been overlooked. Management needs to pay constant attention, and should consider external advice, just as IT management used penetration testing to test security resilience.
- Failures are no longer binary. Datacenters used to be single sites, and the workloads that were sited there were either running or not running. Increasingly, however, applications are distributed, running across multiple sites, calling in remote services. This means failures are often partial, with some components running well, others badly or not at all. This can cause some systems to fail, others to lack key data. This makes diagnosis and resolution difficult; it can also cause contractual disputes.
- Failures are likely to be noticed. Most datacenters, especially colocation companies, house many clients and systems, including many operated by service providers that, in turn, have many clients. Failures will be noticed quickly, and social networking will ensure that competitors and press are alerted. Failures are now both an operational matter and a reputational issue. Ironically, one of those affected by the Fujitsu USA failure was the Financial Conduct Authority – which says that responsibility for failures cannot be outsourced – it has in the past fined companies heavily for IT failures.