DELTA AND SOUTHWEST OUTAGES ARE REMINDERS OF THE IMPORTANCE OF REDUNDANCY AND DISASTER RECOVERY/BUSINESS CONTINUITY PLANNING

Kevin DiLallo, LB3
Joe Schmidt, TC2

August 16, 2016

The news about Delta Airlines' recent catastrophic system-wide failure, on the heels of a similarly devastating failure of Southwest Airlines' computing systems, provides a stark reminder of the importance of investing in redundancy and *meaningful* Disaster Recovery/Business Continuity ("DR/BC") plans. In other words, there's no time like the present to determine whether your critical infrastructure is vulnerable to a single point of failure and, if it is, to dispassionately examine whether your failover plan will actually deliver business continuity. These lessons learned from Delta's and Southwest's misfortune is something that all companies, regardless of industry, must heed or they too could find themselves vulnerable to catastrophic failures.

To be fair, system failures happen every day in large, complex networks. Backhoes take out access circuits, air conditioning stops working in server rooms, routers break, software patches don't work as expected. But there's a significant and painful difference between a failure and a *catastrophic failure.* Companies that have rock solid redundancy and resiliency built into the solutions they buy are able to keep their businesses running and their users immunized from failures. In Delta's and Southwest's cases however, seemingly preventable breakdowns caused massive business disruption and widespread customer frustration, and cost each airline millions of dollars (over $54M in Southwest's case and in Delta's case the dollars are still mounting). The bottom line is that the losses for the airlines were many times more than it would have cost if they had implemented effective DR/BC plans.

It's hard to beat physical diversity (not just of circuits, but of entire data centers) to protect against business shutdowns caused by natural disasters, power failures, and other major calamities. In this case, "physical diversity" means locating redundant data centers in different regions so that a derecho or Super Storm Sandy on the east coast of the United States won't take down your operations across the globe. Although the cost of redundant facilities should always be a consideration, that cost should be balanced against the much greater potential cost (in real dollars, lost trust, and diminished brand equity) of a system-wide failure.

New networking technologies, such as hybrid WANs and Software Defined Networking (SDN), are enabling enterprises to design more flexible and reliable solutions to help protect against catastrophic failures. Companies that can't afford to build and buy physical diversity, or those that don't have the internal resources to design, build, deploy,

and manage a resilient solution are increasingly using cloud-based platforms run by third parties such as Amazon, Microsoft, or Google. These cloud service providers give companies access to highly reliable, resilient, and diverse infrastructure while providing around-the-clock support.

Redundancy and diversity of systems is just one aspect of a reliable DR/BC plan. All too often, companies draft their DR/BC plans as if the odds of ever needing it are more remote than winning the Powerball jackpot. That is, rather than addressing specific "what if's" the plans speak in generalities, objectives, goals, and stakeholders. Those high-level generalities don't provide the guidance the IT department and other operational groups will need if they have to cutover from one data center to another. Drafting a meaningful DR/BC plan requires actually anticipating what could possibly go wrong and then figuring out (and putting down on paper) Plan B.

A DR/BC plan for an enterprise is similar to a personal health insurance policy. The DR/BC plan protects against unplanned events, as does an insurance policy, and the best time to buy the policy is when you're healthy. Take the time now when your network is running smoothly to evaluate your network design and assess your DR/BC plan. If they need updating, do it when you're in control, not when a catastrophe forces you to make unplanned, pressured, and likely, expensive decisions.

LB3 and TC2 counsel clients on network and systems design, redundancy, diversity, and Disaster Recovery/Business Continuity planning. If you would like to knock around some ideas with us, give us a call.

Kevin DiLallo **202-857-2560**
Joe Schmidt **610-241-6167**