The Irony of Cloud Security and Airplanes

By Ronny Loew, National Sales Director for ProCirrus Technologies Inc.

The bottom line: You are in more control and more secure by working with a reputable cloud service firm.

They say that when it comes to statistics, there are those you find and those you make up. Finding statistics around the rapidly growing area of cloud computing is challenging given the many different business models and unique characteristics of the user firms. Recently, Dell completed their Global Technology Adoption Index report which surveyed IT leaders from 2,038 midsized organizations across multiple industries. The gist of the survey is that cloud computing is effective but security concerns remain the primary barrier to its adoption.

Here are a few of the key findings.

There is a correlation of business growth to cloud computing. Of those using cloud, 72 percent of organizations surveyed experienced 6 percent growth or more in the last three years. This is in sharp contrast with companies not using cloud, where just 24 percent have growth rates of 6 percent or more.

Adopting cloud computing improved performance through a better allocation of IT resources (44 percent), cost savings (42 percent) and efficiency (40 percent).

The number one barrier to adoption is security. IT decision-makers still consider security the biggest barrier for using cloud computing (52 percent) and expanding mobility technologies (44 percent).

This survey wasn't specific to the legal sector, however concern around security strikes a chord with my empirical experience.   Often times, concerns around security are actually a perceived of a loss of control. This is especially true since security, like costs, can actually be improved by cloud computing. As I write this piece, from 36,000 feet over Montana, while connected to my office via in-flight WIFI, it's impossible not to be struck by the obvious irony…

Security concerns are the primary barrier to cloud adoption yet Cloud Computing is more secure.

According to my rudimentary and unscientific poll, 80% of people feel safer driving a car than flying a plane. In every case, they say the reason is that they "feel more in control."   Yet, according to the National Safety Council your odds of dying in a car are 1 in 492 but nearly 1 in 8,327 in plane.   Flying in a plane you have a crew of professional pilots with dozens of years of experience at the controls. You ride in a plane that is religiously maintained and tracked throughout its entire life by certified professionals. You are flying in an air space actively managed by a dedicated system designed to keep you safe. Yet somehow we feel safer sharing the roads with those to text, apply make-up and read at 60 MPH.

Why? Well perhaps it's because when planes crash its big news and you will hear about it. How many of the thirty-thousand or so car fatalities did you hear about in 2014? The same applies to with data security. When a major retailer gets breached its headline news for days. How often do we hear about the 600,000 laptops that get lost or stolen not to mention the countless cell phones and thumb drives?

Legal information is by definition privileged and sensitive. A small to mid-sized firm cannot cost-effectively achieve the levels of security required by today's security demands on their own - but they can by leveraging a solid cloud provider combined with a robust internal security policy.

The growth of cloud service providers is a tremendous advantage for the professional service firm as it increases options, drives down cost and, perhaps most importantly, provides greater inter-vendor mobility. A reputable cloud provider will provide the contractual and operational assurances that you are the sole owner of your data and that you may migrate from their cloud platform at your discretion. If you are not satisfied, you have the power to move.

So it boils down to this.

You may access your data from SSAE 16 data centers with multiple levels of physical, electronic and operational security. You can have your servers and applications *flown* by professionals with physical redundancy, real-time backup and customizable disaster recovery plans. You can have your mobile devices encrypted, access your critical data from any internet connection and provide your users with robust end user support. Or… You can keep running with scissors from that dusty, insecure server in the closet and see how that goes.