5 Ways to AVOID Turbulence in 'The Cloud'

The leader of a business considering a journey into the unsettled world of cloud computing could take a lesson from a pilot. Those who fly rely on flight dispatchers to help them avoid turbulence. That's because the dispatcher's vantage point, equipment and training provide a vision the pilot lacks.

Silly comparison?

Only if the CEO has already had a conversation about employees using Dropbox on mobile devices. And only if top leaders know what a "deemed export" is and realize that the business **could be fined $1 million for sending it somewhere it should not have gone. In fact, the most important things to know about cloud computing are things that most users do NOT know.**

Almost anyone who uses a computer has used "the cloud" and almost all users would agree that cloud computing is not only efficient and necessary, it also can be simple and safe. Just like a pilot, however, businesses sometimes require guidance.

In simplest terms, cloud computing involves the storage of data and/or operation of software on servers that are not at your physical location and can be accessed over the Internet. For example, said Baylor law and business professor David Henry, "This can involve all my files and software, where the servers may be in Dallas, while I am in Waco." Henry, himself a pilot, is a patent attorney who lives in Waco but works worldwide. His arrangement is a simple one, and this kind of computing is not a problem for most businesses.

Bigger issues arise when the servers are in another country, or workers use a service like Google Drive to share company documents – and no one knows that they are doing it or what the risks are. This is something the IT department should be managing, said John Tripp, an assistant professor who teaches a Baylor Management Information Systems course that all business majors must take.

"The great benefit of the cloud is that as soon as a business identifies a need, and a corresponding cloud service that can address it, the company can bring the service in – without the need to establish infrastructure, train internal staff, and install and configure the technology locally," Tripp said. However, many IT departments are so focused on keeping day-to-day operations running that they are unable to respond quickly to the business's needs. This leads business users to take matters into their own hands, and the IT department may be unaware that confidential information is being shared in the cloud.

There's also a body of law about what technologies can be shared legally in the cloud. Henry, who teaches patent and trademark law and integrates intellectual property subjects into courses at Baylor's Hankamer School of Business, said he deals with many companies whose executives are stunned when they discover how easily they could violate U.S. export control laws. These laws govern the exporting of certain items and technology – including through so-called "deemed exports" – that involve merely sharing controlled technology with a U.S.-based employee who happens to be of foreign citizenship.

Business executives might discount the risks because they do not export any goods and have no intent to commit a crime. "They think that as long as they are not sending things out for sale, they are not exporting," said Henry.

They would be wrong. Henry offered, in addition to the example of deemed exports, that of the business that stores information and data considered export-controlled technology in a cloud computing system with servers outside the United States. "Even sophisticated companies are often completely unaware of U.S. export control laws in many contexts," Henry said. "In my experience, a minority of companies are fully aware of laws, the scope of controlled technologies, and the applicability of export control laws to things like mere data." The result of running afoul of the laws, even unintentionally, can include sanctions and huge fines.

Businesses can and do use cloud computing legally and ethically, however. Lawyers, for example, now file court documents electronically that used to be hand-delivered. Tripp uses cloud-based reference management for his writing, and cloud-based telecommunications to make conference calls with his research co-authors. Businesses and organizations use cloud-based computing to back up computers and store large documents for easy employee sharing.

But with intellectual property providing most of a business's value, thinking through certain issues regarding how computers and other devices are used can help protect business practitioners and their employees.

bbr.baylor.edu/turbulence-in-the-cloud

Here are ideas for SAFEGUARDING information and avoiding legal pitfalls:

1. Store sensitive data onsite. This data can be anything from controlled technology to confidential client information to intellectual property.

2. Ensure that someone who understands the technology and terminology thoroughly reviews the provider's terms of use to make sure the service conforms to a business's ethical standards. Remember that some cloud services host data farms outside the United States, meaning that merely storing information on such systems may amount to a prohibited export, and that some terms of service allow the provider to divulge anything stored on the provider's server if the provider is served with a subpoena.

3. Train employees about the services they can use on mobile devices and home computers. "In many corporations, the use of the cloud is not visible to the people tasked with ensuring content security," Tripp said. "When anyone in your network can install Dropbox or Google Drive and start sharing files with anyone in the world, the enterprise can be caught out of compliance pretty quickly."

4. Use the skills of your IT department. While cloud services are easy to use, usually without IT assistance, these departments are often full of visionary people who can advance business operations if given a chance, said Tripp.

5. Understand that intellectual property often represents the majority of the value of the business and don't put it at risk. "Unlike Baylor, most business schools barely touch on the topic," Henry said. "Lawyers and business people are often aghast at how IP laws work when compared with widespread and starkly differing beliefs." Tripp noted that future cloud computing will enable companies to purchase IT infrastructure the same way they now pay for electricity. "In other words, metered for, and charged by use." While this will decrease the need for internal IT staff to keep day-to-day operations running, it will increase the need for IT departments to function as advisers and coordinators that utilize a collage of cloud services to build and enable new business value. "The cloud is here to stay. Training users as to the proper use of these tools will go further than trying to put a finger in every hole in the enterprise data dam. At some point, you run out of fingers."