Church leaders are being tasked with making “cloud” decisions, but they need to know whether their decisions are good or bad, wise or unwise. This article will give you a framework for working through cloud decisions.

What is the cloud? There are many ways to define the cloud, which makes listening to most IT experts a challenge when they talk about this topic. Some refer to accessible data and applications (apps), some refer to datacenters (warehouses full of servers), some say it has to do with types of processors, and some say it’s all about being green.

All of that may be true, but a church manager needs to know that the cloud refers to data and applications hosted on a server that is accessed via the Internet. Technically, the server can be in an off-site datacenter, or it can be in your building.

So, what’s the big deal about the cloud? The cloud is a game-changer for those who use computers and mobile devices. It’s as big of a game-changer as was the PC, Windows, and the Internet. It will impact how you and your team do ministry, and how you budget for IT in your church. The good news is that, implemented strategically, it will save your church time and money, and will help you focus on your mission.

What should go in the cloud? Most already have websites in the cloud, many have social media sites, and some are putting their email and data in the cloud. While

the answer to that question may seem obvious to some, it’s important to understand that there are basically two parts to the cloud, and to understand what should go in which part.

Public cloud. When most of us think about the cloud, we think about its public side. The public cloud refers to servers and services that anyone can access. It’s where we put our websites, where we engage in social media, and share photos and videos.

Private cloud. The private cloud refers to servers and services the general public cannot access. These are usually servers and services one must be pre-authorized to access and are usually not discoverable by the general public. This is where church email, voice over Internet protocol (VoIP), and data servers should be. As corporate America is moving into the cloud, it is doing so in the private side to protect sensitive data and communications, and that is what churches should also be doing.

The challenge. Many are advising that organizations put into the public side of the cloud what should be in the private side. For the most part, they don’t understand the fiduciary responsibilities associated with managing a church or ministry, and the risk of being in the public cloud.

The problem is that the data put in the public cloud can be less secure than it should be, and not as secure as a church needs it to be. That may not be the right place for a church’s sensitive data and communications. Consider, for example, what could happen if the following types of data were available to the public at large:

• Congregant or donor database information (contact information or contribution information)
• Sensitive inter-office communications about personnel, and constituents
• Data files such as minutes and HR files

If a church is going to adopt cloud strategies, these types of data must be kept private. Thus, they are best held in the private side of the cloud. That means seeking out a hosting vendor that can keep your private data private.

How do I know our data is safe in the cloud? Corporate America is a good place to look for this answer because those leading large corporations usually have a good grip on their fiduciary responsibility to protect their company’s data. When I researched what their trends are, I found that they are moving their own servers to the cloud rather than relying on generally available services (public cloud). That doesn’t mean data in the public cloud can’t be safe, but it takes extra measures and, unfortunately, leans heavily on the users’ work habits.

If you choose to move your servers into the cloud, the data on them will be at least as safe as if they were in a server room on your premises—probably more so! Using best practices on those servers, like those you would if the servers were local (strong
Nick Nicholaou is president of MBS, a consulting firm specializing in church and ministry IT and CPA services. You can reach Nick via email (nick@mbsinc.com) and may want to check out his firm’s website (www.mbsinc.com) and his blog at http://ministry-it.blogspot.com.

So, what’s the cloud’s advantage? That is a wise question! Adopting cloud strategies can reduce personnel costs and the need to make large capital investments in hardware, software, and engineering. Though the cost will likely be the same as a well-implemented network strategy over 3-4 years time, it outsources the cost of buying, engineering, supporting, and maintaining the servers and services at the core of your local area network. It reduces—and often eliminates—the need to employ IT staff above simple help desk functions.

In a January 12, 2004, Fortune Magazine interview, Peter Drucker, the father of modern management, said, “The inefficiency of knowledge workers is partly the legacy of the 19th-century belief that a modern company tries to do everything for itself. Now, thank God, we’ve discovered outsourcing, but I would also say we don’t yet really know how to do outsourcing well.”

The cloud, strategically done, is wise outsourcing. It helps churches focus on what they’ve been called to do, and eliminates the distraction that having unnecessary IT responsibility brings.

Choosing a Private Cloud Vendor

When looking for a private cloud vendor, focus on these three things:

- **Expertise.** Look for a vendor that is already providing the services you’re looking for. If a vendor wants to charge you to create the technology you seek, look to see if there is someone already providing a similar solution so first you have a sense they can deliver.

- **Vendor sensitive to your mission.** As a church or ministry, you won’t typically call for support yelling, screaming, and threatening lawsuits. But if you’re considering a vendor whose primary focus is for-profit organizations, that is what you’re competing with. Find a vendor who will prioritize your softly spoken requests.

- **The datacenter.** Datacenters boast various ratings. Redundancy and security are the hallmarks of a good datacenter.
  - Tier 1 has no redundancies (up to 28.8 hours of downtime annually)
  - Tier 2 has partial redundancy (up to 22.0 hours of downtime annually)
  - Tier 3 has full redundancy (N+1, up to 1.6 hours of downtime annually)
  - Tier 4 is completely fault tolerant (2N+1, up to 2.4 minutes of downtime annually)