THE CHURCH NETWORK™
Don't Go It Alone.

The Cloud – Changing Everything!

Presented by: Nick B. Nicholaou, President
MBS, Inc. (www.mbsinc.com)
Email: nick@mbsinc.com
Twitter: @mbsnick

Workshop Premise

The Cloud is changing everything we do! And the changes are just beginning for most churches.

What do you need to know about The Cloud? How will it change what you do in your church?

We'll answer those questions and more to help you prepare and to strategically implement cloud computing in your church in ways that help fulfill your ministry vision.

The Cloud – Defined

The Cloud refers to

- _____ data and programs reside, and
- _____ they're accessed

- Understanding The Cloud
  - Hardware platform and operating system _____

Data Network Strategies

Most who engineer data networks

- Focus the _____ on the network servers
- Run many applications, like Church Management Databases (ChMS), from network servers
- Make the network accessible via the Internet

Why Is Corp America Cautious?

Three Dominating Reasons

1. Security & Trust
2. Reliability of Internet
3. IT Directors Protecting their _____

Two Main Cloud Types

'_____' Cloud

- Cloud services that run on servers generally available to any and all interested in the service
  - Google Apps, Yahoo, Dropbox, Facebook, Twitter

'_____' Cloud

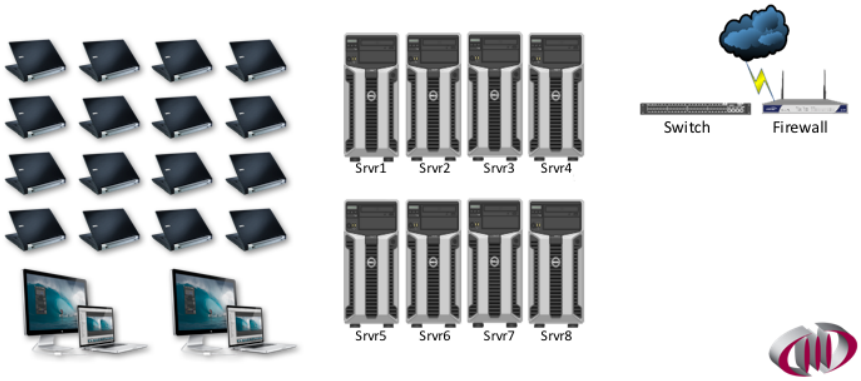
- Cloud services that run on servers generally unavailable to the public
- Server access is secured to only allow those who are _____ to use them

Popular Cloud Services

- Communication Services
  - Email
  - Instant Messaging & Chat
  - Social Networking
- Websites
- Databases
- Data Storage
  - Photos
  - Documents

- Which Should Be Private?
  - _____
  - Instant Messaging & Chat
  - Databases
  - _____ Storage

How The Cloud Simplifies IT



Cloud Pros & Cons

Pros

- No (or *nearly* no) _____
- IT is outsourced
- Saves salaries & capital expenditure planning
- You're no longer responsible for disaster recovery & business continuity
- Accessible from anywhere on almost any connected device

Cons

- Outside of your _____
- IT vendor may not be loyal to your _____
- Might not save money in the long run, but is easier to budget (monthly)
- Your data is somewhere else... can feel like a vulnerability
- No connection, no access– period

What to Look for in a Host

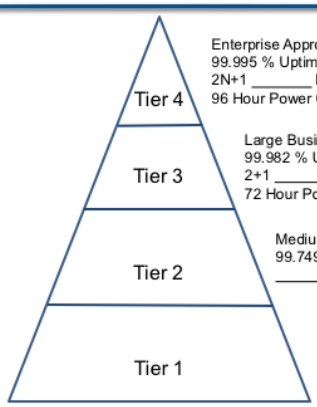
Vendor

- Expertise
- Sensitive to your mission
- Proven track record serving ministries

Datacenter

- Redundancy
  - Power
  - Connectivity
  - HVAC
- Data locations
  - Multiple regional locations, depending on the datacenter
  - All located in _____

Datacenter Ratings



Enterprise Appropriate
99.995 % Uptime (less than _____ downtime annually)
2N+1 _____ Redundant
96 Hour Power Outage Protection

Large Business Appropriate
99.982 % Uptime (up to _____ downtime annually)
2+1 _____ Redundant
72 Hour Power Outage Protection

Medium-Size Business Appropriate
99.749 % Uptime (up to _____ downtime annually)
_____ Redundant in Power & Cooling

Small Business Appropriate
99.671 % Uptime (up to _____ downtime annually)
___ Redundancy

Online Backup & File Synchronization

- Your Data
  - Who _____ it?
  - If you switch providers, what's the process to retrieve it *and* _____ it from their _____?
- Online Backup Examples
  - Carbonite, Mozy, Crashplan, etc
- File Synchronization Examples
  - Dropbox, _____, OneDrive

Wise Cloud Strategies

President, Ministry Business Services, Inc.

Reprinted from ECFA's *Focus on Church Accountability*

Church and ministry leaders are being tasked with making *Cloud* decisions, but need to know whether their decisions are good or bad, wise or unwise. This brief 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 challenging 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 what a church or ministry manager needs to know is that *The Cloud* refers to the fact that data and applications are hosted on a server that computers and mobile devices can access 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 organization. The good news is that, implemented strategically, it will save your organization 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*. And while the answer to that question may seem obvious to some, it's important to understand that there are basically two halves to *The Cloud*, and to understand what should go in which half.

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, and it's where we put our websites, where we engage in social media, and share photos and videos. It includes services such as Google Apps and Dropbox.

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 corporate email, 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; that is what churches and ministries should also be doing.

The Challenge

Many are advising and recommending that organizations put what should be in the private side of *The Cloud* into the public 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.

For instance, there is a movement by many to use Google Apps and Dropbox because of their low cost. 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 corporation needs it to be. Those may not be the right places for a corporation'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 info, contribution info, etc),
- Sensitive inter-office communications about personnel, constituents, etc,
- Data files such as minutes, HR files, etc.

If an organization 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 passwords, good firewall, etc), your data should be safe. If you choose to use public cloud services, have a conversation with your IT person and check with the service provider to make certain all appropriate safety measures are in place.

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 and ministries focus on what they've been called to do, and eliminates the distraction that having unnecessary IT responsibility brings.

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.

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 you have a sense they can deliver first.
- *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)

Back It Up! Here's How…

President, Ministry Business Services, Inc.

Reprinted from *Christian Computing Magazine*

I see this question in IT forums and get asked it a lot: What do you recommend for a backup strategy? The reason is that backup is one of every IT department's highest responsibilities. In fact, a poor or untested backup strategy has caused more IT people to lose their job than any other single issue I've seen. So let's look at the current state of backup best practices.

Backup Strategy

The strategy should be designed to accomplish the disaster recovery and business continuity goals set by an organization's leadership in case a catastrophic event hits. So let's start there.

Most organizations have not stated their goals in this area other than to communicate that the system must be backed up and available ASAP. What does that mean? And what does it cost? And what's the difference between disaster recovery and business continuity?

Simply stated, disaster recovery is the ability to recover from a catastrophic event, while business continuity is the ability to continue to function through such an event. Some data and services are necessary to continue to do business while an event is ongoing. These usually include communications (voice and email systems) and database (ability to look people up, process payroll, etc). It probably is not necessary to have every document or graphic file available to continue to be viable during a prolonged crisis.

That said, leadership should be asked to prioritize the categories of data and services and then state the amount of downtime it considers acceptable during a prolonged event for each category. For instance, they may say that communications should not go down, database should be down for no more than four hours, and the rest must be backed up and available within four business days. That kind of statement should drive the backup strategy, and by categorizing and prioritizing data and services, can help keep the cost of an effective strategy minimal. Not stating recovery and continuity in those kind of terms is usually interpreted by IT that *everything* must be quickly recoverable, and that is a more expensive strategy to implement.

It is also important to point out that an untested backup strategy is, likely, a failed strategy. I've seen many times when good IT people have lost the trust of their leadership because a backup strategy failed when it was most needed— during a catastrophic event. This is an area where being too busy due to understaffing, etc does not work as a reason for not testing the strategy on a periodic basis. Plan to test a different aspect of your backup strategy every month; your team will thank you if it is ever put to a real-time test.

What Solutions Should We Use?

There are many backup solutions available to choose from, and understanding their strengths and weaknesses can help you customize your strategy to accomplish the goals set by leadership within a reasonable budget. If the budget is more than leadership is willing or able to fund, ask them to re-state the disaster recovery/ business continuity goals so you can adjust the strategy accordingly. Their job is to protect the organization and to give you guidance, and it's okay to not get it right in the first pass.

Corporate America is still focused primarily on local tape backups. They are quickly available when a file or folder recovery is needed, and have large enough capacities to cover the full range of data that needs to be safeguarded. Most of our clients purchase LTO4 tape drives, which have 800gb native capacities. For those with larger needs, LTO5 and LTO6 are also available (1.5tb and 2.5tb native capacities, respectively). We recommend doing a full backup nightly, and taking one tape off-site weekly to protect against the loss of a building.

Some today believe that hard drives are better backup targets than tape, but their drawbacks are higher sensitivity to breakage/ failure and higher cost.

Backups require software to make them work, and the solution we have found to be the most capable and reliable is Symantec's BackupExec. It requires more time and attention to keep running well than we'd like (it occasionally drops communication between the backup server and the source, or file server), but we haven't found as reliable a solution yet to replace it that is also reasonable in cost.

What About Online Backups?

The abundance of online backup solutions has, more than anything else, added confusion to the backup strategy discussion. The concept sounds great, and like hard drives sounds like it is a leap forward in technology. However, it has a weakness that cannot be overlooked.

Consider, for example, the amount of bandwidth available at your organization. If there was an event which took out your servers, we could get something up and running in their place within hours. The next step would be to restore data and services. Given the amount of data you have backed up, how long would it take to download your online backup over your Internet connection? If yours is like most churches or ministries, it could easily take a month or more.

To be fair, some online backup organizations say they can send you a copy of your online backup on a tape or hard drive. We have not seen that successfully meet the expectations of IT or leadership. Online backup may be good as a consumer solution, but is not a good enterprise solution.

Nick Nicholaou is president of MBS, an IT consulting firm specializing in church and ministry computer networks, VoIP, and private cloud hosted services. You can reach Nick at 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.

Disaster Recovery & Business Continuity

President, Ministry Business Services, Inc.

Reprinted from *Ministry Tech Magazine*

Most in IT recognize the importance of data backups, but there's more to a good disaster recovery and business continuity strategy than having backups. What are those additional elements, and how do you set an appropriate budget to accomplish them?

Disaster Recovery *vs* Business Continuity

According to Wikipedia:

- *Disaster Recovery Plan (DRP)*. A disaster recovery plan is a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster. Such a plan… specifies procedures an organization is to follow in the event of a disaster.
- *Business Continuity Plan (BCP)*. A business continuity plan is a plan to continue operations if a place of business is affected by different levels of disaster which can be localized short term disasters, to days long building wide problems, to a permanent loss of a building.

When a fire takes out your server room, that's a disaster! Having good backups is an essential element of recovering. In fact, many say that one of IT's most important responsibilities is ensuring good backups.

When a natural disaster like a hurricane or earthquake eliminates the ability to do business as usual for an extended period of time, that's when the business continuity plan kicks in. In the wake of 9/11 and Katrina were many organizations that went out of business because they couldn't continue their operations for a longer period of time than was survivable.

What's Needed for Disaster Recovery?

A good DRP starts with a good backup strategy, and that relies on the ability to reach all of an organization's data. One of the benefits of local area networks is their ability to centralize data, making comprehensive backups possible. With the advent of BYOD (Bring Your Own Device) this is becoming more challenging if staff doesn't do their part to make certain that all organizational data is on one of the organization's servers that is getting backed up.

There are many backup strategies in play today; everything from full hourly to daily incremental backups on backup storage media from tape to removable hard drives to the Internet. I prefer full daily data backups, and agree with most of corporate America that tape is an optimally reliable backup target. Tapes can handle very large backups, and are easily transportable so one can be taken off site regularly (I recommend at least weekly).

What about backing up to the Internet? Though it has advantages, it also has disadvantages; primarily when entire servers need to be restored due to a larger catastrophe. When a large restoration is required, you are dependent on the speed of your internet connection or having the vendor send you the backup. It is worth noting that I've never seen that methodology meet expectations when a large catastrophe hits.

The key to having a good backup, however, is regular testing. This is something most IT teams rarely prioritize. An untested backup is a risk, and there's nothing worse than being in the middle of a catastrophe and running what amounts to your first backup strategy test and finding out that it wasn't working. Our firm recommends doing test restorations on a monthly basis to make certain backups are good.

What's Needed for Business Continuity?

Business continuity requires a larger set of strategies than disaster recovery. In addition to having a DRP component, it needs to include what an acceptable data outage is for different categories of data (email, databases, documents, etc). And it needs to include details on how to respond to different types of disasters including key staff contacts, key vendor contacts, etc.

This is one of the most overlooked needs to good church and ministry administration. In major disasters, churches and ministries want to be resources those in their community can turn to. A BCP helps ensure that your organization will be available to be the hands and feet of Jesus when people need you most.

The Internet can be a good component of a BCP. If you move some or all of your servers and services to datacenters, the likelihood they will not be available is dramatically diminished if the datacenter is certified at least as a Tier III datacenter by www.ColocationAmerica.com.

Setting an Appropriate Budget

The first step is to categorize your data and services (email, VoIP, databases, documents, spreadsheets, audio/ video files, etc). Then ask leadership to set acceptable outages for each category in a disaster. For those categories with very little tolerance for outages (email and databases, perhaps), they need to be backed up in full often and tested regularly. For those located in areas more prone to natural disasters, a good option is to host those mission critical servers and services in an appropriate datacenter. If you choose that option, require the hosting datacenter to provide certification of having a Tier III or higher rating by www.ColocationAmerica.com.

If leadership requires that everything be up and running 24•7, design a plan and budget to accomplish that. If it's too expensive, help them think through the data categories and establish realistic outage timeframes to reduce the cost. But this is a decision that *leadership* must make; it cannot be delegated to IT. And it requires that they agree to the final strategy.

Nick Nicholaou is president of MBS, an IT consulting firm specializing in church and ministry computer networks, VoIP, and private cloud hosted services. You can reach Nick at 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.

MBS, Inc.
MINISTRY BUSINESS SERVICES, Inc.

"…freeing those in ministry from business distractions."

BIOGRAPHICAL SKETCH: Nick B. Nicholaou

Nick Nicholaou is President of MBS, Inc., a team of IT strategists who evaluate, engineer, and support servers, Mac & Windows computers, and mobile devices. In MBS' private cloud datacenter they host Exchange email, SQL databases, VoIP phone systems, SPAM filtering, and file storage/ synchronization.

While in executive service for the auto manufacturing industry, he and his wife Grace sensed God's call to found MBS. Since 1986 Nick and his team have focused on serving Christian churches and ministries nationwide. His specific areas of expertise include organizational management, crisis resolution, and strategic implementation of technology.

Nick has been honored by:
- The Church Network, inducting him into their Hall of Fame.
- Christian Leadership Alliance for his role in assisting ministries nationwide.
- Christian Leadership Alliance with their Distinguished Service Award for excellence in serving ministries.

Nick has been published in print hundreds of times.

- In books
  - Church Finance
  - Business Management in the Local Church
  - The Church Leader's Answer Book
  - Church and Nonprofit Organization Tax & Financial Guide (1999 - 2007 editions)
  - Saving Money And Buying Smart
  - Leadership Handbooks of Practical Theology, Volume 3
- Quoted in ZiffDavis' *eWeek* and *LAN Times*
- In journals
  - *Christian Computing Magazine*
  - CTI's *Christianity Today*, *Leadership Journal*, and *Your Church* Magazines
  - NACBA's *Ledger* and *Insight* Magazines
  - ECFA's *Focus*
  - CLA's *CMA Report* and *Outcomes* Magazines
  - *The Clergy Journal*
  - *Church Business*

He has been interviewed on syndicated radio and podcasts, and is a former member of the ECFA (Evangelical Council for Financial Accountability) Standards Committee.

Nick and his team have served thousands of Christian churches and ministries nationally, and he speaks on a regular basis at national and regional conferences from coast to coast.

Nick's Contact Info:
714.840.5900, x525
nick@mbsinc.com

Blog: http://ministry-it.blogspot.com
Website: www.mbsinc.com