Risk in the Cloud

By Erin Gloeckner

Resource Type: Articles

Topic: Data Privacy, Tech Risk, Cybersecurity

Remember the craze over beanie babies in the 1990s? I was just a kid during the 90s, so I innocently endorsed that craze. My parents suffered through my childhood, spending heaps of money when I demanded to have the next bear, skunk, or whale in my collection. Dozens of cute, colorful animals named ‘Binksy’ or ‘Bubbles’ littered my bedroom bookshelf. Beanie babies were a money pit and I didn’t even know how to play with them. You might feel the same way about technology fads; you spend half a paycheck on the latest gadget, and feel duped when it winds up collecting dust on a shelf.

The latest buzzword in the world of technology is ‘cloud computing’. Cloud computing has existed for more years than many nonprofit leaders realize. But leaders are only recently starting to think about risk when they contemplate the rewards of embracing the cloud.

What Does ‘Cloud’ Mean, Anyway?

The term ‘cloud’ is used to describe any service that is housed by a vendor instead of residing on the servers of the organization using the application or service. For example, the company Rackspace provides data storage infrastructure; Rackspace owns an inventory of servers with rentable space available for clients who need to store digital data. As a Rackspace customer, your nonprofit stores digital data on distant servers instead of storing on the equipment in your own building. Your data is therefore in the cloud.

‘Cloud’ is also used to describe software and platforms. You can use cloud software instead of installing software on your computer. Google Apps provides cloud software including Google Docs, Gmail, and Google Calendar. Instead of using calendar software that is located on your computer’s hard drive, you can use Google Calendar, which is hosted by Google on a far-away server. You never have to download it to use it; you simply log in to the cloud-application hosted by Google.

Forecast: Cloudy with a Chance of Risk

There are a wide range of risks associated with cloud computing, many of which come from user error rather than the technology itself. Yes, you should be worried about information security and data breaches from outside parties. But before worrying over risks in the cloud, make sure your feet are planted firmly on the ground.

During the March 2013 webinar on “Risk in the Cloud,” hosted by the Nonprofit Risk Management Center, guests David Linthicum of Blue Mountain Labs and Matt Prevost of Philadelphia Insurance Companies explained why nonprofit leaders often stumble during their climb to the cloud. Avoid these common failures as you ascend to the cloud:

- **Falling prey to the HYPE**. David Linthicum believes that many nonprofits falter because their expectations of the cloud are unrealistic. There is so much hype surrounding the cloud that we mistakenly think cloud computing is a cure to our technology and budget woes. Instead of accepting the hype as true for your nonprofit, take the time to decide whether cloud computing opportunities are right for you. David also warns nonprofits to complete their due diligence on cloud service providers. If a provider sounds too good to be true, they may indeed be.
- **Trying to fly with NO PLANNING or EXPERIENCE**. David says another mistake nonprofits make is embracing cloud services and applications without vital technical knowledge or experience. If your nonprofit doesn’t have a tech-wiz on staff, then David suggests you get help from an expert. He also encourages nonprofits to complete a few key steps before transitioning to the cloud:
    - Test your new cloud technology on one system before moving everything to the cloud.
    - Consider testing a non-critical system first, rather than testing your cloud with data that is critical to your mission.
    - Contemplate how the cloud will impact and integrate into existing structures and processes at your nonprofit.
    - Recognize the cloud’s impact on your core strategies as well as existing security protocols.
- **Failing to anticipate the risk of DATA BREACHES**. Matt Prevost warns us to focus on safeguarding specific information stored in the cloud, namely: personal health information, personally identifiable information, financial information, and intellectual property. Be sure to protect the information of your clients and donors as well as that of your employees, board members, and volunteers.

Before you choose to abandon some or all of your in-house servers or installed applications, take the time to understand the protection from financial losses available through cyber insurance policies. Most importantly, don’t assume that existing property and casualty policies will cover new exposures arising from your activity in the cloud. Matt explains that most traditional property, liability, and crime policies do not cover damage to data and cyber systems. Your nonprofit may require cyber insurance to cover losses including: cyber extortion, **“Don’t assume that existing property and casualty policies will cover new exposures arising from your activity in the cloud.”** business interruption due to digital malfunction, loss of digital assets, loss of electronic intellectual property, or a compromise of network privacy or employee privacy. Luckily, some cloud service providers also offer cyber insurance. Depending on your needs, it may be more effective to purchase coverage from an outside provider.

Avoid Rain Clouds by Screening Cloud Service Providers

Never be shy about questioning cloud candidates. Before they buy in, smart nonprofit leaders compare potential cloud service providers. Ask very specific questions and check references for any new vendor. Never assume that a vendor will protect your interests financially or otherwise if they make a mistake or something goes wrong. Remember to ask the following questions of your cloud service candidates:

- What is the provider’s response time when the cloud servers go down? What is the estimated ‘uptime’ it will take to get things working?
- Will my nonprofit still have ownership of electronic documents and property that we store in the cloud? What are our owner rights and responsibilities?
- Does the provider offer a warranty? Does the provider have limited liability if we experience a data breach or other loss?
- What is the provider’s dispute resolution process?
- Has the provider acted in consistency with other agreements they have entered into?
- What are the provider’s payment terms?

A Remedy for Cloud Fever

Ask yourself these questions before making the jump to the cloud:

- How is my nonprofit exposed to risks in the cloud? What are the major categories of risk?
- Have other nonprofits stumbled when moving to the cloud? How can my nonprofit keep from making the same mistakes?
- What type of cyber security options are available to protect our cloud data?
- What role might insurance play in the event a downside cyber risk materializes?
- How have other nonprofits fared after transitioning from in-house servers to cloud servers?
- Are all of our staff prepared to access information in the cloud, or are some staff at risk of being stranded on the ground?
- Is our nonprofit jumping on the cloud computing bandwagon just to keep up with the trend?
- Do we have staff members who actually understand the technical aspects of cloud computing?
- Are we prepared to experience cultural and procedural shifts as we rely more heavily on cloud services?
- Have we ever felt disenchanted after adopting the latest IT craze? Why wasn’t the previous technology craze useful to us?
- What are our requirements? What systems do we want to move to the cloud? Do we want infrastructure, a platform, software, a network, or all of those things from a cloud provider?