Nonprofit
Risk Management
Center

Cloud Computing – BCP Boon or Boobytrap?

By Katharine Nesslage

Resource Type: Articles

Topic: Business Continuity Planning, Data Privacy, Tech Risk, Cybersecurity

(download The Business Continuity Planning issue of *Risk Management Essentials*, here.)

Many nonprofits are routinely taking advantage of the “Cloud” to provide low-cost software and data solutions. Gone are the days when organizations were required to purchase and maintain expensive servers on-site to house their applications and data. The allure of being able to remotely access files and web applications from any computer makes the Cloud appear to be an easy remedy for business continuity issues. But is it?

Your nonprofit’s essential information includes the tools and data necessary to continue mission-critical functions during an interruption. When exploring cloud computing solutions, consider the following questions:

- How are passwords and account numbers stored?
- Are multiple individuals able to access systems using unique logins?
- Is the solution likely to reduce friction for maintaining critical functions?
- How do you ensure that account permissions transfer to other people if the initial points of contact are unavailable?
- Who is responsible for maintaining the confidentiality, integrity, and availability of your nonprofit’s information?
- Who is responsible for providing overall cybersecurity for data transfers, and at what level? Meaning, who is securing the server, and what security is implemented when a user accesses that server remotely? (VPN tunnel, encryption keys, etc.)
- Do you know how your outsourced solutions are managing business continuity concerns?

What is The Cloud?

For this article, we use the term ‘the cloud’ to describe a subscription service that primarily delivers ‘software as a service’ (email, calendaring, office tools, etc.), but can also deliver ‘infrastructure as a service’ and ‘platform as a service.’

For a summary of the different types of cloud services visit: “SaaS vs PaaS vs IaaS: What’s The Difference and How To Choose,” BMC Blogs

Applications and infrastructure that are available remotely are examples of cloud computing. Traditional IT assets were housed on physical servers within your organization’s facilities—remember those server closets? Physical hardware has limitations on the amount of data that can be stored, and hardware can be damaged or rendered inaccessible during a power outage or other event affecting your facilities. Many sources state the best strategy for protecting your data and accessing it during an interruption is to put it in the cloud.

Cloud services are useful as they may be deployed rapidly, are scalable, and require minimal upfront investments. And because of the self-service nature of many of these services, they may save you money and time.

Misconceptions About the Cloud

Unfortunately, the concept of “the cloud” leads to a false sense of security that your data will always be intact and available, as long as you can connect to the internet. Using cloud technology as a way of safeguarding your nonprofit’s information and protecting continuity of services requires a careful review of service level agreements (SLA) and your vendor’s BCP practices.

The cloud is “always on.” Because of its high reliability, cloud outages are rare. It’s easy to believe that the data stored remotely is continuously available and automatically protected for disaster recovery. However, nonprofit leaders exploring cloud solutions should ask the right questions of any potential vendors to determine if that particular cloud solution exercises salient business continuity practices.

For example, at any given moment, your data is being delivered to you from a single data center somewhere. Do you know if the owner of the cloud service is able to quickly move to a new data center? The answer may be no, and if so, you need to confirm your cloud provider’s established timelines and procedures for data relocation.

Keep in mind that not all cloud providers maintain their own physical storage. Some may lease space that may not be in the same geographical location as their offices. So, you could have a U.S. based cloud provider whose leased space is actually in another country. Ask your vendors for the physical location of the server where your data is stored.

Backups happen automatically. Frequently, routine backups are included with cloud services. However, it’s risky to assume that redundancy is automatic or conducted on a schedule that is best suited to your organization. Check with your cloud provider to find out if your service level agreement (SLA) includes backup and recovery of your data and what levels of protection are included with your SLA. Never assume that your data is being automatically backed up. Establish a frequency of backups; for essential data, you may want a backup daily or weekly, especially when this information is accessed and updated often.

Data can be recovered immediately. In the event your nonprofit needs to execute data recovery from cloud backups, you need to know how long backups are stored and how quickly information can be retrieved. Knowing how long backups are retained and if multiple versions of your data are stored will prepare your organization for data recovery plans if primary information becomes corrupt. Some backup storage options take advantage of infrequent access and may have longer restoration times, impacting your ability to come back online after a disruption.

Common terms vendors may use during these discussions include recovery time objective (RTO)—the length of time it takes to get your restored data and applications back up and running—and recovery point objective (RPO)—how frequently your nonprofit’s data needs to be backed up.

The cloud safely stores my data forever. Reliance on a third-party to store, administer, and safeguard your data can be risky. What happens to your data if your cloud provider suddenly shuts down? Will your data be gone forever, or does your SLA include a provision requiring a data dump prior to the vendor shutting down? How much notice will you receive to make preparations to move your data to a new service provider? Does the SLA have restrictions if our organization decides to switch to another provider?

Your provider contracts should include an exit strategy describing the steps (and cost, if applicable) to move the service back in-house or to transfer it to an alternative provider. The plan’s most important aspect is the retrieval and preservation of your nonprofit’s data so that data portability is achieved. Keep in mind that an exit strategy is helpful if you or the provider terminate the contract; that strategy may or may not govern how disruptive events like a service outage or bankruptcy will be handled.

Cloud services can provide an efficient, elegant solution for safeguarding your data and continuing critical operations. The key takeaway is to remember that having candid conversations with technology partners about the terms of their services will ensure that your cloud software and storage arrangements sync with your overall business continuity plan and BCP strategies.