Professor Harsh Jadhav, MBA, serves as Chief of Internal Audit at Alameda County Employees Retirement Association (ACERA) where his department is responsible for providing independent assurance and advisory services designed to improve operational efficiencies and protect against misappropriation of public funds.

Prior to joining ACERA, Harsh worked in various finance and management capacities, including positions with Mirabelle Investments, Ernst & Young, Deloitte & Touche, Intel, and American Express.

Harsh is licensed in California, U.S.A. in 10 various professional fields of accounting and finance and holds a Bachelor’s of Science in Accounting from San Diego State University, and a Masters of Business Administration from California State University, Hayward.

In addition to his position with ACERA, Harsh teaches as an adjunct business professor with the University of Phoenix, University of California, Berkeley, and University of San Francisco, and serves on the Governor’s Cybersecurity Task Force, CalCPA Technology Committee, and the Government Accounting and Audit Committee.

With the increasing volume and sophistication of cybersecurity attacks, companies could face significant business interruption and loss of critical data without an adequate business continuity plan. The article by American leading expert in accounting, finance, audit and cybersecurity Harsh Jadhav explores the criteria to select the right cloud-based vendor, and the steps companies should take to evaluate how cloud-based technology can be used to enhance a company’s disaster recovery plan. The author’s ideas and findings may comprise a great interest to numerous stakeholders in Ukraine, from governmental institutions and companies, to financiers and IT engineers.

Внаслідок збільшення кількості та ускладнення рівня кібер-атак, компаніям, які не мають належного плану протидії, загрожують істотні перебої у веденні бізнесу зі втратою важливих даних. У статті провідного американського експерта з бухгалтерського обліку, фінансів, аудиту та кібербезпеки Харша Джадава досліджено критерії правильного вибору постачальника «хмарних технологій», а також кроки, які компаніям слід здійснити, щоб оцінити, як хмарні технології можуть бути використані для покращення плану аварійного відновлення компанії. Ідеї та висновки автора можуть становити значний інтерес для багатьох сторін в Україні, від державних установ та компаній, до фінансистів та інженерів-фахівців з інформаційних технологій.

IMPLEMENTING AN INCIDENT RESPONSE PLAN USING CLOUD-BASED TECHNOLOGY

Harsh Jadhav, MBA, CPA, CISA, CISM, CITP, CRISC
Chief of Internal Audit, ACERA
University of Phoenix Bay Area Campus,
Silicon Valley, California, U.S.A.

Addressing cybersecurity breaches should be high on the list for business continuity planning (BCP) and disaster recovery (DR). Top concerns for disaster recovery revolve around managing security of sensitive data, ensuring accessibility of the data during and after a crisis, and minimizing downtime. In most cases, utilizing cloud-based technology can be a practical solution to mitigate the impact of cybersecurity threats and ensure the survivability of the business.

As a first step, companies should first determine their Recovery Point Objective (RPO) and the Recovery Time Objective (RTO). RPO refers to how much data a firm could afford to lose measured in increments of time without significantly impacting the business, while RTO specifies the point in time in the future at which a firm must be up and running again. To minimize the recovery time, organizations should identify their critical applications and databases, and determine if they make good candidates for inclusion in a cloud-based design, considering that older legacy applications may not be suitable. The cloud-based solution should allow applications and databases to share data and operate without a significant decrement in speed or operational efficiency.

Other essential considerations would include determining whether to use a dedicated server model or a shared server model, wherein several companies use the same server. Shared server models tend to be more popular as they are less costly, and cloud vendors typically have robust security protocols and network architecture in place to prevent unauthorized access to their client’s data. To weigh the different alternatives and determine which cloud-based solution makes sense, a thorough business impact analysis is necessary to decide on the right course of action. Companies should select a cloud model that supports their system infrastructure requirements.

Cloud services models can be categorized into three types.

Cloud Services Model	**Description**
Infrastructure as a Service (IaaS)	Supports the underlying infrastructure (servers, storage, networks).
Platform as a Service (PaaS)	Allows for software development and application deployment.
Software as a Service (SaaS)	Provides access to software applications and databases via a third-party cloud service provider.

An immediate benefit of implementing a cloud-based solution is the cost savings, as it eliminates the need to rent expensive data center space or replicate hardware in a physical data center. Also, the data backup process is automated through uploads and can be backed up on an hourly basis, to minimize recovery time. Finally, cloud-based solutions provide for a seamless transition from normal operations to a virtual office after a security breach, reducing downtime and loss of data.

Along with the benefits, there are also some risks we need to be aware of. One risk is the potential that more hackers will target cloud providers in the future (*ISACA Identifies Five Cyber Risk Trends for 2016* (2016)). Another risk companies will face is that some cloud service provider will not keep up with the latest security standards or will fail to monitor third-party service providers with access to their client’s data. By achieving ISO 22301 certification, cloud service providers can provide assurance that steps were taken to strengthen their process and procedures to enhance their business resilience in a crisis. Finally, if the firm relies on external third parties who host applications to prepare forms or store client information, then it is essential to ensure the cloud service provider migrates the data to the cloud server on a regular basis.

Cloud-Based Service Provider Checklist

1. **Does the cloud service provider have a solution in place to transfer the data to a secondary data center for temporary access if the primary data center housing is unavailable?**
2. **Are the cloud service provider's internal controls sufficient enough to protect the data in the cloud, and during transmission to and from the cloud server?**
3. **Has the data security been tested from the point of input through to the point of retrieval?**
4. **Does the cloud service provider undergo a periodic Service Organizational Control (SOC 2) review? The purpose of the SOC 2 review is to enable an auditor to independently verify that the cloud service provider has adequate security processes in place to ensure their information systems are secure, available, process data with integrity, and maintain the confidentiality of the data.**
5. **When evaluating shared services, does the cloud service provider partition the firm's data from the other companies on the same servers (i.e., firewalls)?**
6. **Is the backup and recovery process tested by the cloud service provider to ensure the company's data would be safely stored and easily recoverable?**
7. **What happens if the cloud service provider goes out of business or if the company decides to terminate the service agreement?**
8. **How are data breaches and downtimes exceeding the RTO, reported back to the company and are these reporting protocols in compliance with global and local laws and regulations?**
9. **What is the availability of helpdesk support during non-working hours?**

It is clear that there is no one-size-fits-all approach to implementing cloud-based services to meet a company's disaster recovery needs, and in some cases, a cloud-based solution may not work at all. For most companies though, a cloud-based solution can be a useful part of an overall business continuity plan, as long as the business requirements are clearly defined, and any cloud-based components are integrated appropriately. An excellent place to start learning more about the different cloud service models, risks, benefits, and challenges in incorporating cloud-based solutions is the ISACA Guide on Controls and Assurance in the Cloud Using Cobit®5. Other good resources include the National Institute of Standards and Technology (NIST) and ISO 22301.

Reference

ISACA Identifies Five Cyber Risk Trends for 2016. (2016). Retrieved from http://www.isaca.org/About-ISACA/Press-room/News-Releases/2015/Pages/ISACA-Identifies-Five-Cyber-Risk-Trends-for-2016.aspx

Article published: December 12, 2018